Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East

Sharon Magen

The utilization of emerging technologies for purposes of cyber espionage is the cornerstone of this paper. Although many have referred to cyber security risks that are directly connected to the security sphere, national security threats due to economic cyber espionage have not been dealt with to the same extent, and this oversight is rather puzzling. As cyberspace becomes increasingly utilized for espionage purposes, it is imperative to further examine the possibility of exploiting cyberspace for the purpose of espionage specifically in the international arena; economic globalization has made the international economic scene vastly interconnected, thus intensifying the vulnerability of the world economy to possible cyber security breaches.

Keywords: Cyber espionage, economic espionage, globalization, national security

Introduction

The recent usage of emerging technologies for the purposes of cyberattacks or acts of cyber espionage in general and the subsequent threat specifically posed to the national security interests of governments in the economic sphere is the focus of this paper. Although many have examined cybersecurity

Sharon Magen holds a Master's degree in Security Studies from Tel Aviv University and completed her internship at the Institute for National Security Studies (INSS) on China-Israel relations and the Gulf Cooperation Council (GCC).

risks that are directly connected to the security sphere, national security threats posed by cyberattacks or acts of cyber espionage in the economic sphere have not been dealt with to the same extent, and this lack of interest is rather puzzling.

As cyberspace is increasingly being utilized for espionage purposes in various fields, it is imperative to further examine the possibility of exploiting cyberspace specifically for the purpose of espionage in the international economic arena; globalization has made the international economy vastly interconnected, thus making the world economy more vulnerable to possible cybersecurity breaches, with such a breach rendering the possible repercussions on national security interests even more intense and on a much wider scale. This lack of contemporary research on the utilization of cyber means for conducting economic espionage and the subsequent consequences regarding national security has compelled me to examine this subject in this paper.

The growing importance of this phenomenon, in which foreign entities may utilize cyber means for carrying out economic espionage to achieve strategic goals, is the incentive for this research. The growing risk posed to national security by economic cyber espionage, coupled specifically with the economic and political rise of China, rather intensifies the importance of dealing with this issue. As a country seeking to become a game-changer in the global arena, it is highly likely that China—significantly more than other countries—fully engages in cyber espionage in the economic sphere so that it can achieve its goals in other fields, such as in the security and political spheres. This issue should be further studied, in order to determine whether cyber espionage in the economic sphere is a threat posed especially by China, and whether this threat should therefore be taken into consideration when considering integration with Chinese entities.

In this case, foreign governments, through private or state-owned companies, can target certain economies or foreign companies for making an investment. The government will then be able to obtain new technologies—an act that may tip the scale in favor of the investing country, which otherwise would not have been able to receive these technologies.

This phenomenon cements cyber espionage in the economic arena now as an undeniable threat to national security. The United States mostly directs this accusation against China, as Chinese companies, which are mostly state-owned, are suspected of utilizing global cyber and economic integration as a vessel for conducting economic espionage; however, some contend that China is not the only country committing cyber espionage in the economic sector and therefore should not be targeted as such.

All countries today engage in cyber economic espionage to a certain degree; therefore, this paper will question the reason why the United States is spearheading the notion that China conducts gross economic espionage, even though it is maintained that other countries do so as well.

My methodology for examining this theoretical assumption entails the assessment of other countries' approaches toward China's supposed cyber economic espionage intentions. If other countries similarly claim that China is the main source of global cyber economic espionage, even though it has been asserted that other countries take part in such espionage acts as well, it would be vital to clarify the reasons for this type of behavior. In order to assess the attitudes of other countries toward China's cyber economic espionage, I contend that it would be most effective to focus on non-western countries, such as the Middle Eastern countries, which may contribute to a more balanced portrayal of other countries' attitudes toward China's cyber economic espionage intentions.

Consequently, in this paper I examine the approach of select Middle Eastern countries toward China's massive involvement in world trade and the possibility of its gross cyber economic espionage activities as a means of assessing the veracity of Washington's claim. Specifically, I examine the cases of the United Arab Emirates (UAE) and Turkey. The rationalization for choosing these two countries is such; the main nexus that binds Beijing to the Middle East region concerns economic security, as more than half of China's oil and natural gas imports are sourced from the countries of the region.

Regarding the UAE, it is important to note that it is only the third largest economy in the Middle East behind Saudi Arabia and Iran. Being a source of oil and natural gas imports for China but not one of China's principal suppliers, the UAE represents a significant case study in this sense as it cannot be characterized as being overly essential to Chinese interests. Therefore, the UAE's approach to Chinese cyber espionage intentions will not be tilted in favor of Beijing.

In contrast to most other actors in the region, hydrocarbons do not play a big role in Turkey's relations with China, thus making Ankara a meaningful choice for a study of relations with China within the Middle Eastern context.

If so, an outtake on the Turkish possible responses to Chinese alleged cyber economic espionage may provide an original contribution on investigating this matter.

The apprehension that through cyber economic espionage China could access key economic interests in a host country's economy and realize its own interests, regardless of the host country's interests, could propel the UAE and Turkey into taking action against Chinese economic transactions, thus initiating the suspension or cancelation of Chinese-backed investments and so on. In order to measure the approach of the governments of these two countries to possible Chinese cyber economic espionage, I will examine possible objections and restrictions made at a government level toward Chinese economic transactions and Chinese-funded projects within the two countries. Upon presenting a consistent trend of government level objections to projects funded by the Chinese, I contend that this is due to the tangible threat to national security posed by cyber economic espionage, and enabled by economic integration.

This research underlines the imperativeness of the need for further study of global cyber integration and the risks that economic espionage entails. Although global cyber integration may present an opportunity for growth, countries must take into consideration the risk of exposing their economy to cyber economic espionage.

Research on Economic Espionage Using Cyber

According to Mary Ellen Stanley, technological advancements and economic integration have vastly altered the perception of national security in the intelligence sphere, due to wide-ranging cyber economic espionage.[1] Similarly, Matthew Crosston argues that typical international economic activity may constitute an intelligence collecting structure by cyber means, designed to enhance military might.[2] Souvik Saha specifically stresses the US standpoint, which is concerned about the Chinese involvement in economic espionage,

[1] Mary Ellen Stanley, "From China with Love: Espionage in the Age of Foreign Investment," *Brooklyn Journal of International Law* 40, no. 3 (2015): 1033–1079.

[2] Matthew Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry," *International Journal of Intelligence and Counterintelligence* 28, no. 1 (2015): 105–122.

and the undeniable national security threat it poses.[3] Furthermore, Magnus Hjortdal emphasizes that cyberspace is a pivotal element in China's strategy to ascend in the international system, and that one of the key means is by conducting economic espionage to gain strategic advantage.[4]

However, İbrahim Erdoğan argues that cyber economic espionage is an immensely lucrative industry in which all countries participate,[5] and therefore cannot be attributed to one specific country. Furthermore, when it comes specifically to the United States, Duncan Clarke contends that even allies of Washington, such as Israel, have been committing acts of economic espionage against the United States for years. According to Clarke, Israeli intelligence units continue to utilize existing networks for collecting economic intelligence, including computer intrusion,[6] thus rendering redundant the argument that cyber economic espionage against the United States is an act of war spearheaded by its foes. The assertion that many other countries in addition to China commit cyber economic espionage against Washington—including its allies who are not reprimanded—weakens the severity of China's acts and the argument of the US intelligence community that China is indeed at the forefront of cyber economic espionage.

Regarding the integrity of the assessments of the American intelligence agencies, John Yoo contends that US intelligence and national security agencies do not always depict an accurate portrayal of national security threats.[7] In other words, the United States may employ false claims to protect the nation's security, thus arguably sacrificing the integrity of the government's efforts. Robert Bejesky similarly throws into question the reliability of these organizations' assertions; according to Bejesky, allegations that the executive branch may induce intelligence assessments to support the position preferred by the executive branch are not without basis. The Central Intelligence

[3] Souvik Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure to Economic Espionage in the Age of Globalization," *Northwestern Journal of International Law and Business* 33, no. 1 (2012): 199–235.

[4] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 1–24.

[5] İbrahim Erdoğan, "Economic Espionage as a New Form of War in the Post- Cold War Period," *USAK Yearbook of International Politics and Law* no. 2 (2009): 265–282.

[6] Duncan Clarke, "Israel's Economic Espionage in the United States," *Journal of Palestine Studies* 27, no. 4 (1998): 20–35.

[7] John Yoo, "The Legality of the National Security Agency's Bulk Data Surveillance Programs," *Harvard Journal of Law and Public Policy* 37, no. 3 (2014): 901–930.

Agency (CIA), for instance, has a long history of politicizing intelligence; at a conference at Harvard in 2001, a panel of experts deliberating the account of the CIA maintained that the agency does not conduct its role faithfully when it comes to sharing unpleasant truths with the executive branch.[8]

If so, it is feasible to comprehend that even though cyber economic espionage may pose a national security threat, the formal accusation by the United States that China is the main perpetrator of cyber economic espionage may be biased. Although China may be committing acts of economic espionage by using cyber means, it cannot be confirmed at this point that it spearheads this area more than any other country.

Growing Interconnectedness

During the past few decades, technological developments have immensely changed the way that governments perceive national security. Conventional acts of espionage, which can be traced to a certain perceptible entity, have merged significantly with cybersecurity, thus rendering ambiguous the identity of the intelligence threat and exposing new domains in which harmful data collection may occur, such as the global marketplace.[9] Today, the world is moving toward a single global economy, due to financial integration.[10] This current reality of cutting-edge technology and worldwide economic integration has changed the face of espionage and has created a world in which national security can be harmed, inter alia, via cyber means in the global marketplace.

Today there is a need to balance a nation's economic affluence and its national security, as economic globalization may become a vessel for espionage through cyber means—the bedrock of connectivity in today's international market. The key methods through which international economic integration may enable cyber economic espionage are when a foreign, state-owned or government body conducts business in the host country, or when a foreign entity acquires a local business within the country.[11] It can be contended that

[8] Robert Bejesky, "Politicization of Intelligence," *Southern University Law Review* no. 40 (2013): 243–292.

[9] Stanley, "From China with Love: Espionage in the Age of Foreign Investment."

[10] Lucyna Kornecki and Dawna Rhoades, "How FDI Facilitates the Globalization Process and Stimulates Economic Growth in CEE," *Journal of International Business Research* 6, no. 1 (2007): 113–126.

[11] Stanley, "From China with Love: Espionage in the Age of Foreign Investment."

this type of activity is not merely a manifestation of economic policy but also functions as a well-planned intelligence collecting scheme intended to serve as an additional form of competition, in addition to military rivalry.[12] Although it cannot be affirmed that cyber espionage is the main incentive for pursuing economic integration, economic integration makes it possible to conduct cyber espionage activities. Countries may even abuse economic integration in order to conduct cyber economic espionage so that they can enhance their military might.

In this regard, many have claimed that China is leading the sphere of cyber economic espionage.[13] According to this approach, China intends to harness the possibilities of espionage offered by today's worldwide market as a means of enhancing its regional and global supremacy. Washington especially perceives Beijing's intention to commit economic espionage through cyberspace as a dire national security hazard, as China's success in conducting effective economic espionage may translate into a sharp increase in China's potential power relative to the United States. China's current investment policy in economies such as the United States consists of mergers and acquisitions, which enable opportunities for undesirable proliferation of intellectual property and trade secrets to Chinese firms via cyber means.[14]

This type of activity is particularly problematic when Chinese multinational corporations, which are mostly government owned, attempt to purchase American companies with strategic significance or which deal with critical infrastructure and assets. According to recent assessments from the US intelligence community, there is a heightened assertiveness within China's international policies, and as a result, it has resorted to massive cyber economic espionage.[15] Moreover, according to Pentagon reports, China will

[12] Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry."

[13] Stuart Malawer, "Confronting Chinese Economic Cyber Espionage with WTO Litigation," *New York Law Journal*, December 23, 2014.

[14] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," *The Office of the National Counterintelligence Executive*, April 14, 2016, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

[15] Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

continue to aggressively collect sensitive American technological information through cyber espionage.[16]

This assertion that China is the main global source of cyber economic espionage may also serve certain US political policies, rather than represent an accurate status of global cyber economic espionage. Although James Comey, the director of the FBI, had stated in May 2014 that the Chinese government blatantly sought to use cyber espionage to obtain an economic advantage for its state-owned industries, Robert Gates, then former US secretary of defense, openly stated that as many as fifteen countries at that time were conducting economic espionage in order to take possession of American trade secrets and technology,[17] thus shifting the focus from China as the leading perpetrator of this act. Furthermore, it has been contended that the US National Security Agency itself had committed cyber economic espionage activities against France.[18]

Given the circumstances, the main question that arises is why the majority of official American security and intelligence bodies spearhead the notion that China is currently the worldwide source of cyber economic espionage while other sources maintain that other countries have committed cyber economic espionage acts as well, including the United States itself. Although China does not actually lead the global cyber economic espionage, top security and intelligence institutions in the United States promote this claim in order to support the US political needs and policies toward China, whose growing regional and world ascendancy threatens the continuation of Washington's world dominance and strategic might. In other words, China's rise poses a political threat to the United States, a fact which has led to American prosecution of Chinese economic interests.

Another question is whether other countries similarly argue that China is at the global forefront of cyber economic espionage. If other countries equally claim that China is indeed the global leader of cyber economic espionage, then what are the reasons supporting this argument? If other countries contend

[16] Geoff Dyer, "China in 'Economic Espionage'," *Financial Times*, May 19, 2012.

[17] Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage," *The Diplomat*, December 17, 2015, http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/.

[18] "WikiLeaks Reveals NSA's Economic Espionage against France," *Progressive Digital Media Technology News*, Jun 30, 2015, http://search.proquest.com/docview/1692699265?accountid=14765.

that China is the world leader of cyber economic espionage, even though many other countries in fact engage in cyber economic spying, then why do they make this claim? It is my assumption that this is due to security motives, related to China's economic rise and the security threat China poses via its economic growth. This would assist in asserting the assumption that China's rise de facto poses a threat to American strategic interests.

Therefore, it can be argued that the majority of official American security and intelligence bodies do not portray an accurate assessment of the case of global cyber economic espionage as other global actors also engage in cyber economic espionage and no single country spearheads it. However, I contend that the *formal approach* of most of the American intelligence institutions toward China in the cyber economic espionage sphere may be intended to serve the US grand strategy toward China's rise, in the belief that China's growth may threaten American strategic interests.

The hypothesis that the United States has advanced the global notion that China leads in international cyber economic espionage due to political, foreign policy, and security reasons can help clarify the gap between the popular claim within the American intelligence community and other entities regarding China's role in cyber economic espionage. Many contend that China's vast economic growth coupled with its enhancing military capabilities has placed it on a collision course with the United States.[19] As a way of challenging China's rise, the United States has depicted China as having minimal respect for intellectual property, sovereignty, and other critical factors that comprise the bedrock of global trade. International trade serves as China's bread and butter, fueling its growth and ability to expand its military capabilities. If the United States can damage China's ability to conduct global trade by asserting that it promotes cyber economic espionage, it would thus damage Beijing's capabilities in the security sphere.

To better understand the reasons why the United States claims that China leads the global cyber economic espionage, we will now look to the UAE and Turkey to see how they relate to China's massive involvement in world trade and the possibility of its gross cyber economic espionage activities, in order to assess the veracity of Washington's claim.

[19] Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

UAE

The UAE is a federation comprised of seven separate emirates, which together represent the third largest economy in the Middle East behind Saudi Arabia and Iran. The UAE has the seventh largest proven reserves in the world of both oil and gas, and in 2010 China imported 64,500 tons of liquefied natural gas from the UAE valued at more than 23 million dollars. Furthermore, the China Petroleum Engineering and Construction Corporation (CPECC) assisted with the construction of the Abu Dhabi Crude Oil Pipeline Project, which now enables the transport of 1.5 million barrels of crude oil per day from Abu Dhabi's collection point at Habshan to the export terminals at Fujairah. Oil transported through the pipeline bypasses the narrow Strait of Hormuz, which Iran repeatedly has threatened to block if it is attacked militarily. However, it is imperative to point out that the 3.3-billion-dollar project had experienced repeated delays, initiated by the UAE.[20]

Although it had been officially stated that construction problems forced the UAE to delay constructing the pipeline,[21] industry sources close to the project claimed another reason for the delay. Although the CPECC was already preparing to commission the pipeline, the Abu Dhabi Company for Onshore Petroleum Operations (ADCO) was not involved in this initial preparation process, a rather perplexing situation, as it would be expected that ADCO would first have to ensure that the commissioned pipeline design suited its standards prior to commencing production.[22]

The fact that the Chinese began designing the pipeline without the participation and involvement of ADCO—the UAE state firm in charge of the project—conceivably indicates that the Chinese intended to commit a sinister act regarding the construction of the pipes; such pipelines include highly sophisticated control software that can be hacked and even manipulated prior to its assembling. In 2004, for instance, Thomas C. Reed, a US Air Force secretary in the Reagan administration, wrote that the United States had effectively implanted a software trojan horse into computing equipment

[20] Manochehr Dorraj and James English, "The Dragon Nests: China's Energy Engagement of the Middle East," *China Report* 49, no. 1 (2013): 43–67.

[21] "UAE Delays Project to Bypass the Strait of Hormuz," *Al Bawaba*, January 9, 2012, http://www.albawaba.com/business/uae-delays-project-bypass-strait-hormuz-408210.

[22] "UAE Delays Oil Pipeline to Bypass Hormuz to June," *Oil & Gas News*, January 16, 2012, http://search.proquest.com/docview/916274658?accountid=14765.

that the Soviet Union had bought from Canadian suppliers, which was used to control the Trans-Siberian gas pipeline.[23]

If so, it is quite plausible that the Chinese had begun the UAE-commissioned pipeline design without involving ADCO because they had something to hide, such as installing cyber espionage measures. This would not be an isolated incident for the Chinese; in 2013, Michael Hayden, the former head of the CIA, contended that the Chinese telecom giant Huawei was spying for Beijing,[24] which rather solidifies the argument that China indeed utilizes business transactions for conducting cyber espionage. In the case of the Abu Dhabi Crude Oil Pipeline Project, the numerous delays due to the ongoing exclusion of ADCO from the pipeline design process can be explained by the fact that CPECC had engaged in illicit activities during the manufacturing of the pipeline, namely the insertion of cyber espionage measures; however, in this case, even though China had engaged in cyber economic espionage, the UAE only delayed the project and did not opt to cancel it entirely.

Turkey

Although more than half of China's oil and natural gas imports are sourced from the countries of the Middle East region, thus deepening Beijing's dependence on the region, hydrocarbons do not play a pivotal role in Turkey's relations with China. Nonetheless, Turkey is a rising power in the region and has not directly experienced upheavals like the ones that were felt in the Arab world in the past few years; thus, Ankara is still one of Beijing's pivotal partners in the region, in the economic and political spheres alike.[25] Regarding the Turkish government's stance on possible Chinese cyber economic espionage activities, it is important to note that in November 2015, Ankara canceled

[23] John Markoff, "Old Trick Threatens the Newest Weapons," *New York Times*, October 26, 2009, http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all.

[24] "Huawei Spies for China, says Former NSA and CIA Chief Michael Hayden," *Business Insider*, July 19, 2013, http://www.businessinsider.com/huawei-spies-for-china-says-michael-hayden-2013-7.

[25] Altay Atli, "A View from Ankara: Turkey's Relations with China in a Changing Middle East," *Mediterranean Quarterly* 26, no. 1 (2015): 117–136.

a tender of 3.4 billion dollars for a long-range missile defense system, provisionally awarded to a Chinese state-owned firm in 2013.[26]

Turkey had originally entered negotiations in 2013 with the China Precision Machinery Import-Export Corporation (CPMIEC) to finalize the billion-dollar contract. Even though the French-Italian consortium Eurosam and the American-listed Raytheon had also submitted offers, the Turkish government preferred talks with the Chinese company, which raised serious concerns over the compatibility of CPMIEC's systems with NATO's missile defenses, of which Turkey is a member. In its official statement given by a representative from the office of then prime minister Ahmet Davutoğlu, the Turkish government declared that it had canceled the deal with China mainly because Turkey had decided to launch its own missile project.[27]

Although the Turkish government officially maintained that the core reason for canceling the multibillion-dollar deal with the Chinese firm had been its decision to develop by itself the long-range missile defense system, concrete concerns within the Turkish government about Chinese cyber economic espionage may have led to the cancelation. As previously stated, Turkey had implemented a comprehensive process for choosing a foreign company to lead this project. If Turkey had indeed wished to self-develop this defense system, it would have done so from the beginning and would not have conducted a complete procedure for choosing a foreign firm to conduct this project.

In other words, it can be argued that after Turkey had decided to continue with CPMIEC in order to further this project, the Turkish government began to express serious concerns regarding possible exposure of sensitive NATO systems to the Chinese. Although the deal did not explicitly address the direct exposure of critical and classified systems to the Chinese, this transaction could have enabled Chinese access to systems through which harmful data collection could be conducted. Transactions such as this may inadvertently enable foreign penetration via cyber means, as foreign firms gain access and exposure to computerized systems through which such infiltration may be

[26] "Turkey Says 'yes' to China's Trade Initiative, 'no' to its Missiles," *South China Morning Post*, November 15, 2015, http://www.scmp.com/news/china/diplomacy-defence/article/1879097/turkey-says-yes-chinas-trade-initiative-no-its-missiles.

[27] "Turkey Cancels $3.4 Bln Missile Deal with China," *French Chamber of Commerce and Industry in China*, November, 15 2015, http://www.ccifc.org/fr/single-news/n/turkey-cancels-34-bln-missile-deal-with-china/.

conducted. Such harmful data collecting activities through cyber means—enabled by seemingly innocent business transactions—are especially perilous when these transactions involve critical infrastructure of the host country.

Although it can be argued that other motives caused the Turkish government to call-off the collaboration with the Chinese state-owned firm, such as the formal Turkish response that Turkey had decided to develop the long-range missile defense system itself, this argument, as stated, is problematic to comprehend as Turkey had already initiated a long process of selecting a foreign contractor. If so, it can be claimed that the Chinese cyber economic espionage threat was a pivotal motive in Turkey's decision to call off the deal, as it is perceived as a real danger by the Turkish government to its national security.

It is apparent that while the UAE and Turkey do not share Washington's vehement concern for the threat of Chinese cyber economic espionage, they do understand the possibility of a threat, as reflected by canceling or delaying business transactions with Chinese firms. Although neither of these countries have exclaimed—as the Americans have—that China uses cyber means as a means of carrying out economic espionage, their behavior toward major Chinese investments indicates that they understand, at least at the government level, that China's economic conduct differs from that of other countries and poses a heightened threat of cyber economic espionage.

The UAE and Turkey are not engaged in great power politics that characterize the United States and therefore lack the incentive as well as the protective means to denounce China's economic conduct. Although there is some government-level resistance to major business transactions with Chinese firms, it mainly occurs through inconspicuous "soft" methods such as project suspension; however, project suspension, coupled with cancelation of business transactions with Chinese firms, forms a stable foundation for the argument that Chinese business transactions specifically are not treated the same as transactions done with firms from other countries, therefore indicating that they pose a threat.

Nonetheless, given that the anti-China steps within the economic sphere are mostly discreet, it is speculative to assume that they are taken in light of China's intentions to engage in cyber economic espionage. Even when these two governments publicly announced the suspension or cancelation of Chinese-funded projects, they did not state that this was due to misconduct rooted in cyber economic espionage. The indication that Chinese economic conduct is treated differently than economic transactions originating from other countries may also further solidify the American claim that China's economic behavior is not innocent; if the governments of Turkey and the UAE believed that China was innocent, they would not publicly announce the suspension or cancelation of major Chinese-funded projects in both countries.

In the literature review section of this paper, I noted Crosston's approach, who states that typical types of international economic activity may constitute an intelligence-collecting structure, designed to enhance military might. Additionally, according to Saha, recent assessments from the US intelligence community contend that China's international policies reflect an intensified decisiveness, and as part of this, China has resorted to substantial cyber economic espionage. The focus of China's business transactions and economic integration in the infrastructure, energy, and telecommunication sectors—all critical to national security—may indeed suggest that the Chinese intend to utilize cyber means for gaining information for their own strategic purposes. The suspension and cancelation of key Chinese-funded projects, prima facie due to technical reasons, suggest that these governments see further Chinese economic involvement in their countries as a threat.

Conclusion

In conclusion, it is possible to comprehend how global cyber interconnectedness and economic integration have affected a country's perception of its national security. While pertaining to be of economic nature only, typical international economic activities may constitute an intelligence-collecting structure, done through cyber means, and intended to aid in enhancing a nation's power. International economic conduct may facilitate opportunities for the proliferation of economic intelligence transmitted to the investing country via cyber espionage, thus compromising the national security of the country that receives the investments. The American claim that China currently spearheads cyber economic espionage worldwide through economic integration has been substantiated by other governments as well, in addition to the reaction of the governments of Turkey and the UAE to business transactions with Chinese firms. Although these countries' reaction is not as intense and straightforward as that of the American government, it is nevertheless apparent that they are striving to restrict or monitor Chinese investments, at the very least.

This research sought to answer why official American intelligence bodies claim that China is currently the main perpetrator of cyber economic espionage, even though other sources maintain that additional countries also commit economic espionage. Given the findings regarding the UAE and Turkey, it can be contended that the United States makes this claim because Chinese investments are perceived as a national security threat, a notion shared by other countries. As seen in the cases of Turkey and the UAE, the delay or suspension of Chinese projects point to the fact that business transactions with Chinese firms are indeed looked upon by these countries—and not only by the United States—as a source of peril, even though it could be said that China is no different than any other country when it comes to economic integration and cyber economic espionage.

This research has contributed to the further study of cyber interconnectedness, alongside economic integration and the espionage risk it entails. Even though the global market place has become increasingly interconnected via cyber means, countries must take into consideration the risk of exposing their country to national security risks, given that international economic integration may prove to be a vessel for cyber economic espionage. Indeed, the United States is not exaggerating when it describes the cyber economic espionage intentions of the Chinese; rather, as a superpower, it is one of the few countries that have the prerogative to openly state its opinion on the matter. It is therefore critical to assess Chinese business transactions differently than those from other countries, given the fact that the Chinese specifically use economic integration for conducting cyber espionage and enhancing Beijing's military and strategic might along the path in its rise.

As further research, I suggest monitoring the response of other powerhouses, such as the European Union and Russia, to China's cyber economic espionage acts, since the notion of China as the global leader of cyber economic espionage prevails within countries other than the United States. In the case of Russia, for instance, it is possible that the Russian government will not publicly support the claim regarding Chinese cyber economic espionage acts in order to solidify the Chinese position vis-à-vis that of the United States. However, the Russian government may also elect to use covert measures, thus protecting itself from the vast cyber economic espionage threat posed by China but in a discreet way, which neither harms its relations with Beijing nor supports the US agenda.

If the other great powers besides the United States perceive China's cyber economic espionage as a central threat to their national security, it would be vital to determine how this would affect world politics and trade. Although some of the great powers today use subtle measures to counter Chinese cyber economic espionage, in the future, as China continues to rise economically and militarily, these countries will have to join forces in order to contain China. To put an end to Chinese cyber economic espionage, the great powers may have to erect international cyber monitoring structures in the economic sphere as a means of decreasing the possibility of international cyber economic espionage.

The British Response to Threats in Cyberspace

Daniel Cohen

The cyber threat ranks high among the risks to a country's interests and national security. In recent years, this threat has already materialized in cyberattacks on political institutions, political parties, organizations, financial institutions, and critical national infrastructure around the world. In the future, additional risks are expected, particularly to the civilian sector, originating in the Internet of Things. These risks are the result of the growing number of connected devices, most of which are neither secured by the manufacturers nor by the users, and the rise in the number of Denial-of-Service (DoS) attacks on public and private systems that are accompanied by extortion and ransom demands.

This article focuses on cybersecurity efforts in Britain. The inherent gaps between characteristics of the flexible and dynamic British private sector and the needs of the bureaucratic and innately sluggish secret security system have hindered collaborative efforts between the cyber industry in Britain and the security system there, as well knowledge sharing between sectors as is needed today. In response to this situation, the government has undertaken strategic processes in recent years to support subjects relating to technology and innovation, with an emphasis on knowledge-intensive industry and cybersecurity. The objective of these processes has been to contend with the changing dynamics of the cyber threats, while attempting to build a bridge between the British intelligence

Daniel Cohen is a researcher in the Yuval Ne'eman Workshop for Science, Technology and Security and in the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University.

agencies and the private market, in relation to issues of defense, research, and development.

Keywords: Cyber security, Britain, research and development, cyber defense, GCHQ, NCSC, deterrence, international cooperation

Introduction

Britain has a long history of using science and technology for the purposes of national security, and its governments have maintained long-range strategies and policies over the years to support the fields of innovation, technology, and knowledge-intensive industry. The Signals Intelligence Corps (SIGINT), which operated on behalf of the British War Ministry, engaged in intercepting the Germans' transmissions during World War I, while sharing knowledge with their French counterparts. British decoding and intelligence collection efforts expanded considerably during World War II and in 1945, approximately 10,000 employees served in the SIGINT service in Bletchley Park.[1]

The British Government Communications Headquarters (GCHQ) was established during the Cold War and is responsible for SIGINT and technology, cyber, and additional tasks related to Britain's national security. Concurrently, the GCHQ provides guidance to government organizations and critical infrastructure organizations in relation to information systems security. In addition to various operative departments, an advanced research department operates in the GCHQ and engages in a variety of topics, such as network architecture, security, linguistics, artificial intelligence, automated machines, and more.

In 2013, the GCHQ was the focus of public discourse, following the publication of the intelligence commissioner's report on behalf of the British government, which contained recommendations for reforms, new legislation, and processes for regulating possible surveillance and wiretapping by British intelligence and the police. This report emphasized the need to create a bridge between the British intelligence agencies and the private market in relation

[1] See Government Communications Headquarters (GCHQ) website, https://www.gchq-careers.co.uk/about-gchq.html.

to issues of defense, knowledge sharing, and research and development.[2] As part of the restructuring, which was designed to create national cybersecurity capability in the civilian sector, the British government announced the establishment of the National Cyber Security Center (NCSC) in November 2015. The center is to be subordinate to the GCHQ but will bear state responsibility for providing cybersecurity to the entire British society and will constitute an address for advice and support for the economic system, while directly cooperating with academia and international entities. The intention of the British government was to render the security system that contends with cyber threats more accessible and capable of cooperating with the private sector in order to share knowledge and resources.[3]

British Government Funding of Technological Research and Development

Over the last three decades, the British government has reduced its investments in research and development. In 2012, for example, the investments in research and development were about 1.72 percent of the British GDP, compared to about 2 percent of the GDP at the end of the 1980s. This figure is also lower than the average of EU member states, which was 2.06 percent in 2012.[4] In 2014, the British government set a target increase in state investments in research and development to 3 percent of the GDP by the year 2020.[5]

Today, the majority of investments in technology and innovation in Britain are allocated to encourage the private sector and not the public sector. The government budgeting for science and research reaches about GBP 4.6

[2] Intelligence Services Commissioner, *Report of the Intelligence Services Commissioner for 2013*, June 26, 2014, http://intelligencecommissioner.com/docs/40707_HC304IntelligenceServicesCommissioner_Accessible.pdf.

[3] Royal Society, *Progress and Research in Cybersecurity: Supporting a Resilient and Trustworthy System for the UK*, (The Royal Society, July 2016), p. 37, https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf.

[4] Charlie Edwards and Calum Jeffray, "The Future of Research and Development in the UK's Security and Intelligence Sector," (Occasional Paper, Royal United Services Institute, March 2015), https://rusi.org/publication/occasional-papers/future-research-and-development-uk%E2%80%99s-security-and-intelligence-sector.

[5] National Audit Office, *Research and Development Funding for Science and Technology in the UK*, Memorandum for the House of Commons Science and Technology Committee, June 2013, p. 7.

billion per annum and does not include direct allocations to the security sector (in which there have been budget cuts since 2010). Between 2010–2014, the digital industries in Britain grew by about 32 percent—faster than the British economy—and employment in these industries increased by 2.8 percent, faster than in all other sectors of the economy. In 2015, 86 percent of the households in the country had internet connections and 76 percent shopped online. In 2016, about 56 percent of the adult population in Britain used a digital bank. Today, the digital industry in Britain constitutes about 7 percent of the British economy and employs 5 percent of the workforce.[6] Notwithstanding the increased use of digital space, the British economy has suffered from rising unemployment rates among technology professionals, while, on the other hand, it has a shortage of professionals in the cyber field.[7] The government identified this gap and today aims to deepen the cooperation between the GCHQ and British industry and to contribute to the growth of the cyber market. The value of this market is currently assessed to be about GBP 22 billion, but revenue from exports of cyber products account for only GBP 2 billion.[8]

Due to the threats in cyberspace, the British government in 2011 formulated a National Cyber Security Strategy for 2011–2016 that reflected the need to create an efficient ecosystem in which the government, the security system, academia, industries, and start-up companies would collaborate in order to respond to the growing security needs. Within this framework, the government decided to invest GBP 860 million in the development of a national cyber security plan.

The implementation of this new strategy was reflected initially by establishing cybersecurity bodies, such as the national Computer Emergency Response Team (CERT), creating platforms for knowledge sharing, encouraging cyber studies in academia, and delegating responsibilities among the various bodies in charge of cyber security. Despite some successes, this strategy was

[6] Office for National Statistics, *Internet Access – Households and Individuals: 2015*, http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/ homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06.

[7] "Jammin' in the Capital," *Economist*, June 21, 2014, http://www.economist.com/news/britain/21604591-londons-creative-talents-have-unleashed-wave-innovative-technology-firms-jammin.

[8] Ibid.

unsuccessful in closing the structural gaps between the flexible and dynamic private sector and the needs of the bureaucratic and innately sluggish secret security system. The lack of systemic transparency also impaired efficiency in the cooperative efforts between industry and the security system in Britain and the knowledge sharing between the sectors. During these years, the British national cyber budget was mostly invested in developing state cybersecurity capabilities, including channeling budgets to law-enforcement agencies that were battling organized crime. Relatively smaller budgets were allocated to the private sector, academia, and the education system.[9]

Updating Britain's National Cyber Strategy

The British National Security Strategy, which was published in 2015, defined the cyber threat as one of the most critical threats and as one of the highest risks to British interests.[10] One year later, Britain's National Cyber Strategy for 2016–2021 was published. This document defined cybersecurity as "protection of information systems (software, hardware and related infrastructure), the information contained in these systems and the services that the systems provide, against intrusion by unauthorized parties, damage or improper use, including premeditated damage caused by a system operator, or unintentional damage resulting from noncompliance with security regulations."[11]

The National Cyber Strategy identified the following main threats to British cyberspace:[12]

- **Cybercrime**: Cyber-based crimes are committed using Information and Communications Technology (ICT), when both the attacker and the victim are using ICT tools; the development of malware to commit financial scams, burglary, theft, disruption or deletion of information; "traditional" crimes in which criminals are aided by computers, computer networks,

[9] About three-quarters of the national cyber budget for 2011–2016, which totaled GBP 650 million, were allocated to the GCHQ and to additional security agencies. See National Audit Office, *The UK Cyber Security Strategy: Landscape Review*, February 12, 2013, p. 16, https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

[10] *National Security Strategy and Strategic Defense and Security Review 2015*, November 23, 2015, Cm. 9161, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

[11] HM Government, *National Cyber Security Strategy* 2016–2021, p. 15.

[12] Ibid, p. 18.

or any other type of ICT (such as information theft or fraud); organized cybercrime by criminal organizations, with an emphasis on Russian-speaking organizations based in Eastern Europe.

- **Countries and state-sponsored groups**: There are repeated attempts by groups to infiltrate British information networks who seek to achieve strategic, political, technological, and commercial advantages. The main threats in this context are to government, security, economic, energy, and communications bodies. Only a limited number of countries have the capability to pose a serious threat to Britain, although many other countries are in the process of developing (or purchasing) cyber tools that could pose a threat to Britain in the not-too-distant future. In addition to espionage campaigns, there is a threat of attacking critical infrastructure.
- **Terrorist attacks**: Terrorist groups are conducting activities in cyberspace against British targets, even though their technical capabilities are poor at this stage; nevertheless, even attacks using simple tools have the potential to cause tremendous damage. Most of the threats are website defacement attacks, leaking personal information, and so forth as the objective of the terrorist organizations is to achieve public exposure and to intimidate victims. The frequency of DoS attacks and website defacements are forecasted to rise, coupled with an increased use of insider threats.
- **Hacktivism**: These are groups of activists whose principal attacks are DoS and website defacement. These groups are decentralized and focus their attacks on specific issues and carefully choose their victims.
- **Script kiddies**: These are individuals with limited cyber capabilities who use attack tools developed by others. They do not have the potential to pose a wide-scale threat to the economy and society but do have the potential to cause significant damage to an individual or to an organization.

The British cyber strategy published in 2011 did not achieve the target of securing Britain's digital assets. This situation led the British government to understand that it needed to invest more substantial resources to contend with the changing dynamics of the threats and resulted in the drafting of its vision for 2021, which relies on the approach of the National Cyber Security Strategy. This approach includes four key components: defense, deterrence, development, and international activity, as specified below:[13]

[13] Ibid., p. 15.

Defense: Defense is based on the existing resources in Britain for defending against cyber threats, with the objective of creating an effective response capability and ensuring the proper functioning of networks and information systems. The basic assumption is that Britain must reach its objective, whereby civilians, businesses, and the public service will have the know-how and capability to defend themselves against cyberattacks. To this end, the government will focus its resources, coupled with those of the industry, on developing and implementing the Active Cyber Defense approach (see below) that will minimize the cyberattacks under normal circumstances, including phishing attacks, filtering of malicious IP addresses, and active blocking of malicious activity.[14] The state's capability to thwart these basic types of attack will improve the British defense capability against most of the known cyber threats.

Deterrence: The aim is to fortify the British cyberspace against all forms of aggression, while identifying, understanding, investigating, and thwarting attack attempts. In addition, this involves chasing attackers and prosecuting them, including offensive activity in cyberspace. Britain will convey clear messages to its enemies about the expected outcomes of any threat or attempt to harm its interests or those of its allies in cyberspace.

Development: This is designed to support innovation and the growth of the British cyber industry. Inter alia, at stake is scientific research and development; investing in human resources in the public and private sectors; investing in the training of analysts and experts in relation to future cyber threats; investing in research with a long-range perspective, with the aim of encouraging the development of human capital comprised of academic scholars in the field of cyber.

International activity: Designed to deepen the current cooperative efforts with Britain's neighboring international partners and create new cooperative efforts to build capabilities that will help to secure UK assets throughout the world. These types of cooperation will be achieved through bilateral and multilateral agreements that will include the European Union, NATO, and the UN.

[14] According to the government data, a total of 54,456 cyberattacks have been thwarted since June 2016 (phishing and infecting websites with viruses). About 36 percent of these attacks originate from British IP addresses. 64 percent targeted government websites specifically in order to obtain citizens' personal details from government databases.

The joint report of the National Crime Agency and the National Center for Cyber Security (NCSC), which was published in March 2017, stresses the need for cooperation between industry, government, and law-enforcement agencies in Britain, given the intensifying cyber threat and the rapid changes in this arena. The report focuses on the process whereby criminal elements are learning about how state players attack organizations like financial institutions; the risk of the Internet of Things, given the rise of the number of connected devices, most of which are not secured, neither by the manufacturers nor by the users; and the rise in the number of DoS attacks, accompanied by extortion and ransom demands.[15]

Implementation of the British National Strategy in Cyberspace

In order to achieve the objectives defined in the National Cyber Strategy for 2016–2021, in 2016, the British government decided to invest GBP 1.9 billion in cybersecurity. This decision was reached after a series of strategic cyberattacks on political institutions, political parties, and parliamentary bodies, and the collection of information about British national infrastructure. As an initial step towards improving cybersecurity, the British cyber system was reorganized and the NCSC was established,[16] which was given national operative responsibility over the entire field of defending the cybersecurity in Britain. This responsibility includes, inter alia, knowledge sharing, contending with vulnerabilities, and professional leadership of cybersecurity at the national level. Since the British security system possesses strong capabilities in protecting its internal systems and is required to conduct flexible independent operations, it was decided that the NCSC will cooperate with the military's Cyber Security Operations Center and create an interorganizational platform that will enable the British military to take part in the defense against cyber events that could potentially cause strategic damage at a national scale.

The NCSC was officially launched in October 2016 as part of the GCHQ. The vision behind its establishment was to create a headquarters that would

[15] "The Cyber Threats to UK Businesses, 2016/2017 Report," *NCSC & NCA*, March 14, 2017 http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

[16] "The Launch of the National Cyber Security Center," *National Cyber Security Center*, February 13, 2017, https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre.

manage cyberattacks during emergencies; provide guidance on a routine basis and during states of emergency; serve as a knowledge center for the British cyber community; and constitute the liaison between government and industry. The NCSC became an ecosystem for existing cybersecurity bodies, including the Center for Cyber Assessment, the national CERT, and the GCHQ's Communications-Electronics Security Group, which engaged in information security. Additionally, the new NCSC was delegated the responsibility for all cyber issues that had formerly been under the responsibility of the Center for the Protection of National Infrastructure.

The Defense Perception

The British cyber defense approach is based on the need to devise a state solution for strengthening defense at a national scale and on instructing the industry to formulate security measures for critical national infrastructure in such vital sectors as energy and transportation. The British defense approach is to be realized through cooperation with industry,[17] including outsourcing, with the aim of using autonomous defense techniques to minimize the impact of cyberattacks being committed by hackers and to catch viruses and spam mail before they reach their intended victims. One of the success indicators as defined by the government in this context is the timeframe during which a malicious website distributing malware remains active. In the past, the duration was about one month, compared to only about two days currently. Another indicator is the number of phishing attack websites registered in Britain that have been removed from the web after about one hour, whereas in the past, it took about twenty-four hours until they were removed.

The British defense approach also prescribes that a large portion of the government's investments in cybersecurity be allocated to strengthen the cyber capabilities of the law-enforcement agencies and to create a defense response that would substantially increase the cost of cybercrimes, in addition to forming international cooperative efforts and building offensive cyber capabilities as a response to state attacks against Britain. As part of the

[17] An example of cooperation with the cyber industry is by encouraging the national CERT to form cybersecurity clusters to share and expand the knowledge about cyber defense topics. These clusters are dispersed throughout Britain and operate on an independent, voluntary and informal basis. For the list of clusters, see: https://www.ukcybersecurityforum.com/cyber-security-clusters. HM Government, *National Cyber Security Strategy 2016–2021*, p. 33.

strengthening in these areas, more than fifty cyber researchers and technology experts were recruited for the national cybercrime unit and dozens of millions of GBP were allocated to fight cybercrime.

Active Cyber Defense

In order to implement the security measures needed at the national level, an approach was formulated called Active Cyber Defense (ACD).[18] In the commercial context, the term ACD usually relates to analyses of cybersecurity risks, developing an understanding of the threats on the web, and implementing pro-active measures that are needed as a defense response. In its British National Cyber Strategy, the government opted to implement the commercial approach in a broader context: it will reflect its unique capabilities in order to influence the measures to be taken against the spectrum of cyber threats. According to this approach, "the web" represents the entire British cyberspace at the macro level. To achieve this target and reduce the cyber threats against Britain—including those by organized crime cartels and state entities with malicious intentions—the authority and capabilities of the GCHQ, the Department of Defense, and the National Crime Agency will be expanded.

The success of the ACD approach will be measured according to the following outcomes:[19]

- The establishment of a broad defense system that will hinder attempts at phishing, SMS spoofing, and spoofing attacks as part of social engineering campaigns
- Blocking of malware
- Protecting traffic on the internet and communications networks against rerouting attempts
- Enhancing the capabilities of the GCHQ, the National Crime Agency, and the British military in providing an effective defense response to strategic cyberattacks

Knowledge Sharing

One of the key insights of the British cyber strategy is that most of the attacks are committed using basic attack tools, and correct preparedness by organizations could prevent them. To this end, the GCHQ created a platform

[18] Ibid., p. 33.

[19] Ibid., p. 35.

for knowledge sharing and wrote a user manual called "Cyber Essentials," which is useful mainly for defending small and medium-sized businesses.[20] The National Cyber Security Center also wrote a user manual addressing cyber risk assessment called "Ten Steps to Cyber Security."[21] These courses of action also have regulatory implications pertaining to the definition of the standard by which British organizations should prepare themselves in terms of cyber threats.[22]

Another authority involved in cybersecurity in Britain is the Office of Cyber Security and Information Assurance (OCSIA). Operating at the government level, its roles are to support the cabinet ministries and the National Security Council in relation to all aspects of cyber by offering strategic guidance and coordinating the cybersecurity plans at the government level.[23] OCSIA works in cooperation with government ministries and government agencies, such as the Office of Homeland Security, the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry of Communications, and the GCHQ. OCSIA is also in charge of allocating resources and coordinating between the government ministries on cyber-related issues. It also engages in aspects of cyber policy that interface with the private sector. In the future are plans to establish a body called the Emerging Technology and Innovation Analysis Cell (ETIAC). ETIAC will be tasked with identifying technological developments, threats, and opportunities for national security and government cyber bodies.[24]

Another body tasked with state responsibility on topics relating to cybercrime is the National Cyber Crime Unit (NCCU).[25] The NCCU, which is subordinate to the National Crime Agency, began operating in

[20] HM Government, "Cyber Essentials," http://www.cyberaware.gov.uk/cyberessentials/.

[21] National Cyber Security Center, "10 Steps to Cyber Security," April 10, 2016, https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[22] "Minister for Digital and Culture Matt Hancock's speech at the Cyber Security Institute of Directors Conference in London," March 27, 2017, https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference.

[23] See the OCSIA website: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

[24] It should be noted that a consulting team for strategic thinking, the Secretary's Advisory Group on Horizon Scanning (CSAG), operates in the cabinet.

[25] See details about the agency: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

2013 and leads and coordinates the state response to cybercrimes, including the provision of support to its partners in the security system. The NCCU operates in cooperation with Regional Organized Crime Units, the London Metropolitan Police Cyber-Crime Unit, industrial entities, government bodies, and international law-enforcement units.

The Cyber-Security Information-Sharing Partnership began operating in Britain in 2013. This platform encompasses more than two thousand public organizations and private companies. The British companies and organizations also have access to IBM's X-Force Initiative, which provides more than 700 terabytes of information about cyber threats.[26]

Research and Development

The encouragement of R&D is reflected in the decision to establish cyber innovation centers that advance cyber solutions and constitute infrastructure for the establishment of new cyber companies as well as a foundation to fund cyber innovation, with the support of start-up companies and academic research studies in collaboration with industry. In total, approximately GBP 165 million were allocated within the framework of the 2016 Cyber Strategy to support innovation in the fields of cyber defense and security.[27]

In addition, Britain established the Cyber Security Research Institute that brings together the country's leading universities to engage in strengthening the security of smart devices. The NCSC and the GCHQ support innovation and research on cyber topics for school-age children. One of the programs that the GCHQ funds is the Cyber First Program, with some 2,500 pupils between the ages of 11 and 17 taking part in free cyber courses.[28] The program also includes a cyber competition for girls between the ages of 13 and 15.[29]

Approximately 250 students studying relevant professions in academic frameworks receive annual scholarships valued at GBP 4,000 per annum, with the aim of reaching a total of one thousand students by 2020. The NCSC

[26] Royal Society, *Progress and Research in Cybersecurity*, p. 42.

[27] Ibid., p. 10.

[28] "Applications open for GCHQ's Cyber Summer Schools," *GCHQ*, May 20, 2016, https://www.gchq.gov.uk/press-release/applications-open-gchqs-cyber-summer-schools.

[29] "National Challenge will Develop Schoolgirls' Cyber Security Skills," *GCHQ,* January 18, 2017, https://www.gchq.gov.uk/press-release/national-challenge-will-develop-schoolgirls-cyber-security-skills.

and the GCHQ cooperate with about twenty leading universities throughout Britain in offering twenty courses to master's degree students, whereby the students carry on for an additional year of advanced integrative studies in digital forensics, computer science, and cyber studies. The NCSC also launched several research initiatives, which include a plan for establishing thirteen academic centers of excellence in cybersecurity research and awarding scholarships to thirty PhD students who were selected from the centers of excellence. The NCSC also established the government's Cyber Security Innovation Center, which serves as an incubator for start-up companies.

In 2017, the GCHQ published an RFP for the funding of initiatives and research, and established an accelerator for cyber-related start-up companies.[30] This accelerator program includes, at the initial stage, seven start-up companies that receive support from such corporations as Telefónica and Cisco. The GCHQ's intention is to find start-up companies, such as Cyber Owl, which developed an early-warning system that provides intelligence in real time; Status Today, which developed an artificial-intelligence platform to analyze human behavior in the workplace and prevent attacks from within the organization; and Elemendar, an artificial-intelligence platform for analyzing risk reports.

Another initiative that focuses on government and industry cooperation in funding cyber research studies in academia is the Cyber Invest Program. The British government announced the program in 2015, as part of the cooperation with local industry, with the intent of implementing cyber research studies at the commercial level. This program is part of the GBP 165 million allocated for cyber defense and innovation, with the objective of helping start-up companies reach commercial achievements and helping noncommercial cyber initiatives.[31] In the year following the announcement of the program, eighteen companies undertook to invest GBP 6.5 million in this field over the next five years.

Another cybersecurity research body was established in 2013, the Research Institute in Science of Cyber Security (RISCS).[32] Its purpose is scientific

[30] "The first-ever GCHQ-backed Accelerator Programme for Cyber Security Start-ups Concludes Today, with all Parties Involved Hailing it as a Huge Success," *Wayra,* March 30, 2017, https://wayra.co.uk/first-cyber-security-start-ups-graduate-from-unique-gchq-cyber-accelerator-programme/.

[31] Royal Society, *Progress and Research in Cybersecurity*, p. 60.

[32] See the institute's website: http://www.riscs.org.uk.

development and the creation of standards and action methodologies for decision-makers in the field of cyber. RISCS is funded by the GCHQ and the Engineering and Physical Sciences Research Council.

International Activities

In 2016, Britain funded programs to strengthen the national cyber strength and to support thirty-five projects in about seventy countries worldwide, at the cost of GBP 3.5 million. One of the countries where Britain has joint cyber research programs is Singapore. The joint cybersecurity R&D program between the two countries was launched in 2015, and it includes funding research studies in this field.[33] Since the program was launched, six joint research programs have been operated, at an estimated cost of GBP 2.4 million.[34]

Britain has signed cyber cooperation agreements with the United States, Australia, New Zealand and Canada.[35] Britain's international cooperation in the field of cybercrime is under the responsibility of the National Crime Agency, which maintains connections with Interpol, Europol, and additional agencies.[36] In recent years, British governments have also been promoting strategic cyber-related dialogues with various countries. In 2016, Britain formulated a policy communique with China to deepen the cyber efforts between the two countries, including the design of an intelligence-sharing mechanism, cooperation during states of emergency, and more.[37] During that

[33] See the program's website: https://www.nrf.gov.sg/funding-grants/international-grant-calls/joint-singapore-uk-research-in-cyber-security.

[34] Ankit Panda and Conrad Prince, "On the United Kingdom's Cyber Strategy and Asia," *The Diplomat*, October 15, 2016, http://thediplomat.com/2016/10/conrad-prince-on-the-united-kingdoms-cyber-strategy-and-asia/.

[35] "What is the Five Eyes Intelligence Alliance?," *France 24*, March 17, 2017, http://www.france24.com/en/20170317-what-five-eyes-intelligence-alliance.

[36] "International Cooperation," *The National Crime Agency*, http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership/international-cooperation.

[37] Cabinet Office and Foreign & Commonwealth Office, "China-UK High-Level Security Dialogue: Communique," policy paper, June 13, 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.

same year, the governments of Britain and India published a joint statement about strategic cooperation between them, including in the field of cyber.[38]

Shortcomings in the Implementation of the British Strategy

Despite the substantial increase of the British budget for defending cyberspace for the years 2016–2021 and the reorganization and pooling of the powers of the cyber defense arms in Britain, many challenges and deficiencies still hamper the assimilation and effective implementation of the British cyber strategy. The British government's policy of actively influencing the processes of developing technological innovation in the field of cyber defense requires the creation of balances between the security, technological, economic, and social components. Nonetheless, the security component appears more dominant than the other components and serves as a central axis through which the government operates to create conditions that will enable the development of knowledge and an innovative technological environment. From the defense-security perspective, and particularly given the historic structure of the British security and enforcement system, it is only natural that the GCHQ divisions will coordinate the high-level defense capability. This axis, however, constitutes a disadvantage in all that pertains to the interfaces maintained outside of the British security system, which can assist in the synergies between the security system and the civilian system, such as developing academic knowledge, training high-caliber professionals, reciprocities between industry and academia, business development, and technological innovation. The GCHQ's dominance also impedes Britain in all matters pertaining to cooperation with global technology companies. In other words, the decision of the designers of the British strategic approach to base it on Britain's existing resources for defending against cyber threats creates a built-in failure, which poses challenges to implementing the desired response. This failure is reflected, inter alia, in the lack of significant encouragement provided to global technology companies for promoting development, research, and significant business efforts in Britain.

[38] Prime Minister's Office, "Joint Statement between the Governments of the UK and India," press release, November 7, 2016, https://www.gov.uk/government/news/joint-statement-between-the-governments-of-the-uk-and-india.

In addition, there are those who point to a similarity between the structure and policy of the British cyber system and those of the State of Israel. This comparison has not withstood the test results as it pertains to the difficulties of the British model in enabling an efficient ecosystem encompassing security, industry, education, and academia. For example, Israel maintains a high level of competition in the global cyber market, due to its graduates of technology units in its security system who have established successful companies that provide dual security products designed for both security and civilian use, and/or security technologies for which civilian applications can be found. The relative advantage of the Israeli security system is that it does not necessarily invent the technology but rather adjusts it to civilian developments in the private market according to its needs. On the other hand, the situation in Britain looks different and, in many instances, is even the opposite: the British security system contributes its share to technological development, but only a portion thereof is transferred to the civilian market. Consequently, the British governmental mechanism constrains the local cyber industry's ability to maintain a relative advantage in the reality of global competition and relative to emerging threats. This situation will remain as long as the British government continues to invest most of its cyber defense budget in the agencies charged with this task. One can assume that many resources in the government's cyber defense budget that are allocated to the British security and intelligence agencies, such as the GCHQ, are still being allocated to offensive and not defensive capabilities, and more resources are allocated to defending critical infrastructure than to defending other infrastructure. To close this gap, Britain needs to consider severing the NCSC from the GCHQ, either fully or partially, and turn it into more of a civilian body to which the private sector has access. Britain also needs to better and more fully utilize the exchange of technological information and solutions between the British security sector and civilian industry. A correct way to implement this is by taking a holistic approach that will distribute the resources more evenly between security and investments in education, academia, and the private sector.

Finally, Britain's exit from the European Union is expected to have implications on its national cybersecurity. Britain's exit will apparently lead to its departure from EU organizations, such as the European Cybercrime Center and, consequently, it will no longer be a partner in the European Union's cybercrime prevention efforts. It is not yet clear what Britain's policy will be regarding joint regulatory issues among member states of the European Union, such as the General Data Protection Regulation, and to what extent its policy will change once Britain leaves the European Union.[39] Once it exits the European Union, Britain will have to contend more vigorously with the recruitment of high-caliber manpower for cyber professions. In November 2015, cybersecurity was added to the list of professions that are in short supply in Britain. Consequently, citizens outside of the European Union will be allowed to submit applications for work visas in Britain. Britain's exit from the European Union is liable to lead to the opposite scenario, whereby British cyber professionals will opt to work in other countries (where the income levels and the opportunity of professional mobility will be higher after Brexit). Furthermore, Britain will be forced to find budgetary means to fund academic research in technological fields that today are partially funded from European Union budgets. A short-term solution for this would be to divert resources that were earmarked for research and development and for financing European Union funds in order to open special academic research funds in the British centers of knowledge. On the other hand, Brexit is not expected to adversely affect Britain's strategic cyber partnerships with the "Five Eyes" countries (Australia, Canada, New Zealand, Britain, and the United States).[40]

Conclusion

Britain made a long-range strategic decision about national cybersecurity, which includes strengthening the national resilience in cyberspace in general and in digital space in particular, through government investments designed to create human capital from the school level, including the establishment of centers of excellence in cyber security research and cyber accelerator programs for start-up companies. Some of the resources are be devoted to reorganizing the cyber defense arrangement and to recruiting cyber experts for Britain's law-enforcement authorities and intelligence agencies. The

[39] A resolution within the scope of the GDPR, which is expected to come into effect in the European Union during 2018, requires companies registered in the European Union to notify their governments about cyberattacks against them within 72 hours. See also the European Information Security website: http://www.eugdpr.org.

[40] "The Implications of Brexit on UK Cyber Policy," *Council on Foreign Affairs*, June 28, 2016, https://www.cfr.org/blog/implications-brexit-uk-cyber-policy.

jewel in the crown of Britain's strategy is the establishment of the National Cyber Security Center, which is tasked with building a bridge between the government and industry and with providing guidance and management during states of emergency, including cyberattacks targeting critical national infrastructures.

Alongside building offensive deterrence capabilities, Britain is working towards reducing "basic" cyberattacks in the short-term, which constitute most of the attacks against it. Additionally, Britain formulated a vision whereby topics, such as autonomous systems, the Internet of Things, and smartphones—which will constitute most of the medium-range threats—will already receive a response through the establishment of an academic and commercial research infrastructure that will try to contend with the challenges and threats over time.

Britain's National Cyber Security Strategy for 2016–2021, which received a budget of about GBP 1.9 billion, focuses mainly on implementing the approach of self-reliance on the technological and human resources for the purpose of defense, the creation of deterrence mechanisms, and international cooperative efforts. It appears that, unlike in the past, when the GCHQ and the British security organizations relied on their own systems in all matters pertaining to the fields of security R&D, the current British approach encourages decentralization of capabilities and research and also includes a new strategy, whereby the GCHQ is more open than in the past to cooperation with civilian and public bodies in order to promote technological innovation and to develop human capital and the growth of the British civilian cyber market.

Notwithstanding the efforts exerted to date, many challenges and gaps continue to hinder the assimilation of the British cyber strategy. Among the challenges is the excessive concentration of the British cyber defense structure under the GCHQ and Britain's expected exit from the European Union. A possible solution to these challenges is a more balanced distribution of resources between investing in cybersecurity and investing in education, academia, and the private sector.

Campaign in Cyber or Cyber in the Campaign

Avner Simchoni

The field of cyber has acquired increasing legitimacy as an arena of action, as the international system becomes accustomed to its various uses for a range of needs. Israel sees cyber as a vital component of its national security, requiring investment and nurturing. From a historical point of view, the success of security and intelligence campaigns derives from smartly integrating new fields into the existing fabric—means, methods, and concepts—while implementing the necessary changes and adjustments. With the rapid introduction of cyber elements into our cognizance and systems, it is important to maintain perspective and to realize that while cyber is an important and expanding component, it is not a distinct, independent entity. This becomes even more valid when considering processes of situation assessment and decision making and the use of force in the face of threats on numerous fronts.

Keywords: Situation assessment, decision making, cyber, campaign, use of force, multi-disciplinary, technological revolutions

Background

We are currently at the height of a global trend in which the cyber dimension is becoming a central factor in all areas of life. This centrality creates dependence on cyber within developed countries and advanced economies as a vital pillar, beginning with conduct at the individual level, to economic

Avner Simchoni is a graduate of the Security Studies Program at Tel Aviv University and is a researcher in the fields of security and strategy. The author wishes to thank Brig. Gen. (Res.) Meir Finkel, commander of the Dado Center, for his helpful comments.

systems and how countries treat their citizens, and to its effect on global processes. At the same time, the involvement of cyber and its influence is evident in security and military aspects and increases as more systems are integrated into communications and computing.

Among the more prominent cyber events reported in 2016 were the following:

- attacks on essential infrastructures in Europe, including electricity systems
- attack on the Democratic Party servers in the United States
- attacks on targets in Vietnam
- the Locked Shields international cyber exercise with the participation of NATO states and other countries
- hacking of an electronic commerce system in India and the theft of details of some ten million customers
- the wide-ranging DDoS (distributed denial of service) attack on the American internet service provider DYN, and prolonged interference with activity on many important sites
- hacking and theft of tens of millions of dollars from the Central Bank of Bangladesh by means of the SWIFT mechanism (effective later action led to a considerable reduction of the amount stolen in this incident).[1]

The field of cyber is increasingly becoming a legitimate arena of action, as the international system becomes accustomed to the various uses of cyber for different needs. Governmental entities, or elements with government support, individual hackers, and "private" organizations are also active in the field—although with less intensity—and exploit the problem of attribution

[1] Meir Orbach, "Innovations of the Hackers Develop like Cyber," *Calcalist*, January 24, 2017 (in Hebrew); "President of Central Bank of Bangladesh Quits after 81 Million Dollars were Stolen from Bank Accounts by Hackers," *Globes*, March 15, 2016 (in Hebrew); Jim Finkle, "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued," *Reuters*, April 25, 2016; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016; Kyle York, "Dyn Statement on 10/21/2016 DDoS Attack," *Company News*, October 22, 2016, http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/; "Cyber-terrorists Attack Flight Info Screens at Vietnam's 2 Major Airports," *VnExpress,* July 29, 2016, http://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html; "Locked Shields 2016," *NATO Cooperative Cyber Defense Center of Excellence*, April 18, 2016.

in cyberspace; we currently know of over half a billion malware programs active in cyberspace.

Unlike traditional fields of power, giant network and commercial corporations— mostly American, such as Google, Facebook, Microsoft, Twitter, Amazon, Apple—are also key players in this arena, closely pursued by Chinese companies (such as Huawei, Alibaba, and others). These giant corporations are far from being neutral platforms and have evolved into a kind of "gatekeeper" and new form of consciousness shaper: they are the ones that provide access and determine what the public will see and when, while countries and other international elements have almost no powers of regulation over them. To this, we can add cyber security and protection companies, which along with the internet corporations create a unique cyber environment. The big data revolution and high degree of connectivity resulting from the increasing implementation of IoT devices ("Internet of Things") have also increased awareness and exposure to cyber, as well as the assessment and investment by key players in cyber-related disciplines.

At the same time, diplomatic activity in the UN, NATO and other institutions (including at the bilateral level like the limited non-aggression pact between China and the United States in 2016) is working to formulate international norms and more effective, coordinated ways of handling shared cyber threats. Thus, authorities in the United States and other countries drew up demands for internal regulation of cyber challenges,[2] as well as for strengthening the ability of banks to deal with cyberattacks. At this stage, the focus of these demands is on providing backup and recovery capabilities for financial institutions in the face of serious cyberattacks; indeed, these institutions appear to be leading the private-civilian sector in investing in cyber defense.

According to a survey by the Fahn Kanne & Co. accounting firm, the annual financial damage due to cyber incidents worldwide is estimated at hundreds of billions of dollars.[3] It is also estimated that cyberattacks have reached second place in global financial crime, and they have affected about

[2] Tali Tsipori, "Regulation around the World: Government Dealings with the Cyber Challenges," *Globes*, April 5, 2016 (in Hebrew).

[3] Idan Rabi, "Annual Damage Worldwide caused by Cyberattacks—about 315 Billion Dollars," *Globes*, October 23, 2015 (in Hebrew).

35 percent of companies. Cases involving ransomware attacks rose by some 1000 percent last year, and these attacks are expected to increase.[4]

The targets of cyberattacks are varied: security elements, government and political bodies, the industrial and financial sectors (theft of business information and of money), databases, citizens, and even essential infrastructure.[5] Although it is difficult to quantify the damage caused by cyberattacks from the security-military aspect, it is clear that it is severe, and as a result, security establishments all over the world are investing huge resources to protect their systems. The former head of the CIA, David Petraeus, stated that "hackers are becoming more and more creative and wicked . . . Innovation in the field of hacking is developing like the cyber industry itself."[6]

This article seeks to clarify where Israel stands in relation to these trends, and specifically how Israeli activity in the cyber field should be integrated into the wider context of national security and address threats in the various arenas.

The Situation in Israel

Israel sees cyber as an essential component in its national security. As such, cyber requires continuous investment and nurturing so that Israel can maintain its leading position in the field of cyber on one hand and deal with the growing cyber threats from rivals and enemies on the other hand. This approach was already evident at the beginning of this decade with the National Cyber Venture Committee, led by Prof. Isaac Ben-Israel, who had been appointed by the prime minister. This committee outlined the principles for building an Israeli eco-system to facilitate optimal handling of the challenges of the cyber age. The vision and the goal that were defined in this framework were "to maintain Israel's status in the world as a development center for information technology and to ensure first class capabilities in cyberspace

[4] Aviv Levy, "Cyber Crime Has Climbed to Number 2 in the Economic Crimes in the World," *Globes*, November 8, 2016 (in Hebrew).

[5] Vindi Goel, "Yahoo Says 1 Billion User Accounts Were Hacked," *New York Times,* December 14, 2016.

[6] Orbach, "The Innovation of Hackers is developing like Cyber."

to safeguard its financial and national strength as an open, democratic and knowledge-based society."[7]

Like other countries and organizations, Israel is the target of cyberattacks on a daily basis. These attacks are designed not only to steal information and money but also to interfere with and damage production, management, and control systems. The number of attacks and attempted attacks amount to several thousand per day. A recent survey of 150 organizations in Israel found that a quarter of them had experienced a cyberattack during the previous three years by criminal elements, activists, and terror groups, affecting their routine conduct.[8] According to the Institute of National Security Studies, the cost of cybercrime in Israel is approaching ten billion dollars annually, including several billion dollars of damage from theft of commercial information.[9] Political, security, and other sensitive events are often the catalyst for increased attacks or for implementing latent capabilities in the cyber field.

Israel's lead in the field of cyber is manifested by policy and strategy outlines;[10] the activities of operative elements; the expansion of cooperation with international bodies; the technological development of security and

[7] Isaac Ben-Israel, "The National Cyber Project," *Ministry of Science and Technology*, May 2011. In this context, it is noted that as far back as 2002, Israel recognized in good time—partly thanks to the recommendation and involvement of the National Security Headquarters—the cyber threat to essential infrastructures and set up a special body to deal with these threats. See Yossi Melman, "The National Security Headquarters Will Benefit from the Elections," *Haaretz,* December 13, 2000 (in Hebrew).

[8] Ami Rojkes Dombe, "Half of the Respondents in the Survey 'State of Cyber Protection in Israel' are not Ready for a Cyberattack," *Israel Defense*, no. 29, May 2016 (in Hebrew).

[9] Rabi, "Annual Damage Worldwide Caused by Cyberattacks."

[10] See, for example, Rami Efrati and Lior Yaffe, "This is how to Build a National Cybernetic Defense," *Israel Defense,* August 11, 2012; "Policy of Regulation Cyber Defense Professions in Israel," *National Cyber HQ*, December 31, 2015. Activity in this field also takes place in the academic-research space. See, for example, Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy,* Memorandum 153 (Tel Aviv: Institute of National Security Studies, 2015); Ashton Carter, "Preface by Secretary of Defense," in Department of Defense, "The DoD Cyber Strategy," 2015.

civilian cyber products at the highest level;[11] the broad base of academic knowledge and infrastructure (currently five university research institutes work on the cyber field in Israel); and the training of skilled human capital in scientific disciplines connected to the cyber world and its implementation. There are about 400 cyber companies active in Israel,[12] and in 2015 they exported goods and services valued at billions of dollars, equal to about 10 percent of the total global cyber market. At the same time, Israel allocates—as well as attracts from outside—extensive funding for cyber R&D, which has been consistently rising over the last decade. Israel currently accounts for about 15 percent of total R&D investment worldwide in the field of cyber.[13] It should be noted that these figures change every year, as the global market grows, although Israel has maintained its leading place in both absolute and relative terms. The establishment of the Israeli cyber industry puts Israel in second place worldwide (in absolute terms) after the United States.[14]

The security system, the civilian sphere, and the private market in Israel maintain close mutual ties in the fields of training people and developing cyber skills: students acquire technological and scientific education before their military service; the technological system in the Israel Defense Forces (IDF) and the defense establishment trains and drills many people at the technological front; individuals leaving the defense system continue to advance cyber products and services in the private market and in security industries; and the academic world is working constantly to develop theoretical and practical knowledge. The state's investment, either directly or indirectly through its various arms, is discernible in most of the areas mentioned above.

In recent years, cybernetics has achieved a high status in the country, in accordance with the vision and purpose defined at the National Cybernetic Venture, the prime minister's policy, and decisions by the government and

[11] Prime Minister Benjamin Netanyahu, "Israel—World Cyber Power," *Globes*, April 3, 2016 (in Hebrew). It is also important to remember in this context the trend of advanced technologies and applications that germinate within military systems for meeting operational needs, and that are eventually further developed, and establish themselves in the civilian commercial market. Examples are computers and cellular devices.

[12] "The Israeli Cyber Security Map," *IVC Research Center*, January 2017.

[13] Meir Orbach, "15% of the World Investment in Cyber—in Israel," *Calcalist*, January 26, 2017 (in Hebrew).

[14] Amitai Ziv, "Cyber Power: The Sales of the Israeli Companies—10% of the World Transactions," *The Marker*, May 25, 2015 (in Hebrew).

the IDF. In January 2016, the prime minister stated in public that "cyber creates extensive financial opportunities. We want to be one of the five world cyber powers . . . to be a leader in this field. There are three main aspects of cyber: national, civilian and military . . . The first thing is that we have to immunize organizations and civilians. Every society and every person must be protected. The second thing is defense. [Thirdly,] there are large scale incidents that require a response against the attack and the attacker."[15] The prime minister spoke on this subject in public again, and stated that

> Cyber is linked to every industry today . . . The Internet of Things will create so [many] connections that we'll need a lot of solutions to cope with cyber defense . . . Cyber is also a new arena on the battlefield . . . With one press of a button, a lone hacker can bring a country to its knees. Nearly all the countries' infrastructures and intelligence are exposed to cyberattacks . . . A few years ago, I set an objective for Israel to become a leader in cyber. We have achieved that. We have also opened in research center in Beer Sheba. Israel accounts for about a fifth of global investment in the field of cyber. That's bigger than the population by a factor of 200 . . . We are developing Israel's human capital through training programs in the army and in academe.[16]

As for the growing cyber threat, the prime minister stated: "Terror organizations are using the same tools [that] we use— against us . . . In recent years Iran has been building a terror infrastructure in the Middle East. The Internet of Things can be used by these organizations for dangerous objectives. Unless we work together and cooperate, the future could be very threatening. In this context, Israel, the United States, and other countries must cooperate at government and industrial level."[17]

These understandings and decisions found expression in the allocation of resources; the establishment of new organizations and changes to existing ones; in the attention paid at command and administrative levels; the integration of cyber into theory; and programs for building up and operating forces. Among the steps taken in this context in recent years, we can mentioned the

[15] Raphael Kahan, "Netanyahu's Speech at Cybertech: 'We want to Lead the Field of Cyber Worldwide,'" *Calcalist*, January 26, 2016.

[16] Ami Rojkes Dombe, "Statement of the Prime Minister at the Cybertech Conference," *Israel Defense*, no. 31, January 2017.

[17] Ibid.

formation of the National Cyber Headquarters,[18] the National Authority for Cyber Defense,[19] the cyber setup in the various branches of the IDF,[20] the growing allocation of national resources, development of perceptions, drawing up regulations and implementing procedures,[21] expanding partnerships, and more. The field of cyber is also becoming more important in Israel's other security and intelligence entities and has become part of the mission of each organization.[22] A similar situation is taking place in other parts of the civilian system in Israel, including government ministries, statutory authorities, business entities, and public corporations.

Cyber as a Component of the Whole

The understanding that the future of cyber will be in "almost everything"—blurring traditional boundaries between civilian and defense, private and collective, national and international, the actual and the virtual—creates a challenge for state systems that seek to continue functioning at a high level and therefore require special preparations. In this context, we should mention the recent expansion of the national cyber network, whose purpose is to assist in realizing the national cyber vision and to create an environment that will support Israel's future prosperity and leadership in this field.

However, the profound effect of cyber is evident in other areas of security, intelligence, and the army, with emphasis on issues relating to the operating forces and managing military campaigns. A sufficiently broad historical perspective will show several other revolutions in technology, infrastructure,

[18] Promoting National Capability in Cybernetic Space, Government Resolution 3611, August 7, 2011.

[19] Promoting National Preparation for Cyber Protection, Government Resolution 2444, February 15, 2015.

[20] Gabi Siboni and Meir Elran, "Establishing an IDF Cyber Command," *INSS Insight*, no. 719 (July 8, 2015); Yossi Melman, "A Hole in the Network: Decision of the Commander in Chief not to Create an IDF Cyber Command is a Mistake," *Maariv*, 7 January 2017 (in Hebrew); Yossi Hatoni, Postponing the Establishment of a Cyber Command—A Justified Move," *People & Computers*, January 1, 2017 (in Hebrew).

[21] Promoting National Regulation and Government Lead in Cyber Protection, Government Resolution 2443, February 15, 2015.

[22] Itamar Eichner, "Exposure: Cyber Unit of the GSS from Within," *Ynet*, January 18, 2017 (in Hebrew); Eliran Rubin, "That's How You Missed the Chance to be Hackers in the Mossad," *The Marker*, May 15, 2016 (in Hebrew); Yossi Yehoshua and Reuven Weiss, "Geeks in the Dark," *Yedioth Ahronoth*, February 10, 2017 (in Hebrew).

and concepts that have had a profound and long-lasting influence on the battlefield and the world of intelligence and national security in general. These include weaponry, communications, traffic, data processing, means of collection, and more. The marked influence of cyber on concepts and practices that were commonly used until cyber appeared in its full intensity is essentially no different than the invention of explosives, the telegraph, the railway, the internal combustion engine, or flying.

Looking back, certainly to the start of the twentieth century, we can see that the success of armies and intelligence campaigns was usually the result of smartly integrating new means, methods, and concepts into the existing fabric, while making the necessary changes and adaptations. Examples are the use of railways to transport troops and equipment between fronts; the integration of tanks in battles and for moving over land; the harnessing of the computing revolution to gather information; or creating the capability for in-depth bombing using air forces. At the same time, some security failures were the result (even if not exclusively) of uncontrolled adoption or reliance on “the next new thing”—avant garde—such as the commanders behind the “plasma” screens. Here the intention is not to promote a reactionary or conservative approach that avoids all progress and unavoidable developments but rather to position change or revolution within the broader context.

At this point, I want to argue that it is within the context of the recent welcomed introduction of cyber into various systems (and the potential is still great) that as a historical lesson, we must maintain a broad perspective in all areas of security and intelligence and remember that cyber is just another tool—however large its scope and significance—to add to the constantly changing and existing arsenal. With all its importance and unique characteristics, above all, its immense influence in all areas of communication (interconnectivity), cyber should not be viewed as a distinctive, separate field when it comes to the processes of building and operating forces. Cyber is a multi-disciplinary field and not one-dimensional; it is not just “another technology” but rather a phenomenon with sociological, legal, economic, and other dimensions.[23] The multifaceted nature of cyber strengthens the need to integrate it into the fabric of the total system and not to isolate it.

[23] Yitzhak Ben Israel, “Cyber: Not What You Thought!” *CyberTech 2017*, January 2017, pp. 7–8.

The issue of deterrence in cyber also reflects the need for a holistic view. The problem of attribution makes it difficult to identify the object of deterrence and to adapt the tool for the required objective, although we can assume that the intensity of this problem will decline over time, as protective tools are improved.[24] The desirable answer to this question is that cyber deterrence does not have to remain within the field of cyber ("unique response") but can and should combine financial elements, international norms, and more. Prof. Nye argues that effective deterrence in cyber cannot be generic but rather needs to be adapted to each specific threat.[25] This understanding fits in well with the need to carry out a holistic assessment of a situation, allowing the use of a range of policy tools from different disciplines.

Some see cyber as a component of such enormous potential power (whether within or, as already mentioned, outside the field of cyber) that it can be used to project national strength to the outside world, analogous to a navy that controls the sea, the straits, marine commerce, marine battlegrounds, and more.[26] Perhaps this analogy is more suited to the first days of cyber, when advanced technology in this field seemed to be available only to superpowers; now it seems a little far-reaching, given the rapid proliferation of defensive cyber technology and other technologies. At the same time, this analogy does raise once again the enormous potential of cyber, which extends far beyond its narrow field, in a way that requires global and interdisciplinary observation.

As for the decision-making processes, the General Headquarters at the military level and the National Security Cabinet at the national level are the bodies in Israel responsible for overall observation—the holistic view—and for weighing all the inputs required for an integrative situation assessment as a basis for making decisions about building and using military force. Cyber is just one of the inputs, however great its importance. This is also how to interpret the statement by the prime minister about "large events that require a reaction against the attack and the attacker."[27] It is not correct to conduct an "assessment of the cyber situation" other than as a component of a general

[24] Joseph Nye, "Can Cyber Warfare Be Deterred?" *Project Syndicate*, December 10, 2015.

[25] Ibid.

[26] Joseph Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), p. 4

[27] Kahan, "Netanyahu's Speech at Cybertech."

assessment, just as it is not correct to have a "National Security Council for Cyber" outside the integrated entity that is responsible for assessing the national situation—the National Security Council (NSC).[28] Just as nobody would think of having an "NSC for the Air Force" or a "General Headquarters (GHQ) for the Armored Corps," in addition to the top-level leadership and command personnel, we must be careful of the tendency to manage a "national cyber campaign" as a separate system, rather than always seeing it as part of the wider system of the IDF or any other body, each according to its tasks and powers and all of them together as complementary parts of the entire national security.

It is correct and accepted to have headquarter entities for specific areas, both within the IDF and outside it, but these should be subordinate to the process of situation assessment and making decisions in the GHQ and the cabinet, with inputs from a range of sources, according to the rules of the GHQ as defined in GHQ Orders, in the NSC Law, and in other procedures. A situation in which a body that is responsible for a particular subject, no matter how important, also acts as the superintendent reflects an internal contradiction and raises the risk of interfering with the way top-level bodies should work and make decisions.

The National Information Directorate, established after the Second Lebanon War in 2006, based on the understanding of the importance of the public-media aspect of the campaign, is located in the Prime Minister's Office, but it has no pretensions to replace any of the bodies actively engaged in providing information (the Foreign Ministry, the IDF spokesperson, and so on); the Counter Terrorism Bureau was established in the 1990s in the Prime Minister's Office, and later made subordinate to the NSC, with the purpose of coordinating and improving cross-organizational cooperation in the field of fighting terror—in the face of the growing threat—but not to serve as a replacement for any of the security and intelligence entities. The products and bureaucratic location of these two bodies reflect the understanding that there is a need to strengthen the corporation between various government organsand that these matters need increased attention at the national level.

[28] See the National Security Headquarters Law, 5768–2008, which states that "The National Security Headquarters shall be the headquarters for the Prime Minister and the Government for all foreign and defense matters of the State of Israel" (Section 1b), and among other things shall prepare "an annual and long term assessment of the political-security situation" (Section 2a6).

However, they are not autonomous bodies nor "the last authority" in their fields but rather provide an important input to the integration and decision-making process at the political level, as a part of all the generic processes serving it.

Security entities must also be punctilious about introducing the "cyber input" to the mix of the overall situation assessment process, together with data and other inputs that may crop up, both "traditional" and new, for a complete process. If cyber is indeed "a new arena in the battle field,"[29] as the prime minister said, then the "cyber battle" must be conducted as another one of the battles that together form the campaign and not as a separate campaign. The former head of the CIA, David Petraeus, commented that "cyberattacks have already led to the imposition of sanctions, and it is obvious that we are entering a world where responses will depend on the severity of the damage. I believe that serious long-term damage to electricity systems will lead to a serious response. The response may involve cyber, diplomatic steps, sanctions or even a more serious response."[30] Cyber integrates with, affects, and is affected by other elements; in this situation of mutual links and influences, isolating cyber would be a methodological failure.

The placement of cyber in the correct context is also necessary from the organizational point of view. Since we are still in a relatively early stage of the cyber revolution and its integration into all spheres of life and into security systems, we cannot yet properly know the optimal way of organizing cyber in our systems in the future. Every organization naturally goes through changes over time, and organizational structures are shaped and abandoned based on accumulating experience. Indeed, in recent years various entities have been defining and updating their structure, while on the move, in a positive and necessary process of learning, adjustment, and adaptation. In view of both the objective and subjective difficulty of predicting how the relative position of cyber will be defined as part of the broad picture, it is essential to retain flexibility and a holistic view. Practical experience and learning processes, together with past examples and historical insights, will lead us, hopefully, to the optimal position. We can contribute to this, in terms of processes and organizations, if we ensure a proper balance and exposure

[29] Kahan, "Netanyahu's Speech at Cybertech."

[30] Orbach, "The Innovation of Hackers is Developing like Cyber."

to mutual influences between the various components, which in turn can also help to shape the field of cyber itself.

Conclusion

Cyber is continuing to stimulate profound changes in matters of security, the army, and intelligence. This is all part of its penetration into all systems of our lives and the huge social and economic revolution that accompanies it, which some are comparing to the agricultural, printing, and industrial revolutions, which changed the face of humanity. Cyber undermines traditional systems, and it integrates with contemporary trends that are challenging the existing liberal-democratic order that took root after the Second World War. Cyber is also changing the balance of power and the sources of authority that we have known until now, including concepts of sovereignty, territory, monopoly over the means of violence, and changing the ability to use force. As has already been shown, and according to widely accepted estimates, cyber embodies vast potential, for good and bad, and therefore requires enormous investment of resources and handling by all state entities, in both the national and international arenas. Consequently, the momentum and investment in all aspects of cyber development is inevitable, and it is all the more proper that Israel—through its security and civil organizations—leads the field in raising awareness of this.

At the same time, because of the rapid establishment of cyber in our various systems and as a result of our awareness, we must maintain a proper perspective, in which cyber is an important and growing element but not an independent or distinctive element. These words are even more apposite in relation to the issue of using force in the face of threats in different arenas. Taking a national view that is too narrow could lead to failures in assessing the situation, to organizational distortions, and ultimately even to errors when making decisions. A campaign will always be the result of inputs from a range of sources, creating a winning synergetic effect. Any bias towards a specific area, however important it may be, increases the risk of cognitive failures and mistaken decisions.

Just as a war is made up of a series of efforts and battles in various locations and of different types—sea, land, air, space, different geographical areas, political moves, financial aspects, technological and logistical considerations, and more—where it is the cumulative impact that leads to the final result, so too the world of cyber must be integrated into the total campaign in the political-security field. We must not try to conduct a separate "cyber campaign" that is independently managed but rather work for the smart integration of cyber into the general campaign, with all its considerations and aspects.

We have recently learned that an attack on the servers of the US Democratic Party during the 2016 presidential elections provoked a response (at least partially) in the diplomatic and public arenas. The conclusion is that the kinetic, the cybernetic, the media and the information effort, ground maneuvering, diplomacy, economic power and logistics—all these and others—create together the whole; accordingly, we must relate to all of its parts.

Cyber Threats to Democratic Processes

David Siman-Tov, Gabi Siboni, and Gabrielle Arelle

The Russian interference in the presidential elections in the United States and in France raises questions about the need and ability of democratic countries to protect their election processes. This article indicates the importance of relating to elections in a democratic country as both critical infrastructure and as a critical process, and it presents the threats to elections posed by both cyber and cultural developments. This article addresses the reality in which the extensive use of social networks and direct communications channels enables foreign entities to significantly influence the democratic process—without crippling the voting systems—by introducing outside influence into the political discourse. This constitutes a new challenge to democratic countries, which warrants thinking and re-organization.

Keywords: Elections, cyber, cyber protection, critical infrastructure, social networks, political subversion, information operation

Introduction

The fundamental values of democratic countries are liberty, equality, participation, and civil rights. One of the main characteristics of a democratic country is the holding of general, free elections that take place at intervals as prescribed by law. Elections are the ultimate expression of the democratic process and constitute a key component of building the public's confidence in a country and the faith of its citizens in its institutions.

David Siman-Tov is a researcher at the Institute of National Security Studies. Dr. Gabi Siboni is a senior researcher at the Institute of National Security Studies and heads its Cyber Security Program. Gabrielle Arelle is a research assistant at the Institute of National Security Studies. The authors wish to thank Colonel G. for his contribution to this article.

In recent years, we have seen attempts of external interference and subversion of the election processes in many democratic countries throughout the world through cyberattacks. Cyber threats to the election process in democratic countries may be categorized as threats that aim to disrupt the process through technological tools designed to corrupt information systems and the polling and voting systems, and as material threats to democratic institutions by sullying their good name and by undermining the public's faith in them. While the first category of threats is well known, and countries are well prepared to contend with them, the second—which is more abstract—is a new type of threat that requires appropriate consideration and analysis.

A report by the American intelligence community that was submitted to the US president in January 2017 assessed that Russia conducted an extensive campaign to undermine the chances of Democratic candidate Hillary Clinton and to promote Republican candidate Donald Trump in the 2016 presidential elections, using both covert cyberattacks and overt efforts to influence public opinion. According to the assessment, Russian cyber agents had hacked the Democratic Party's computers already back in July 2015 and used information that they had collected during this intrusion.[1] This incident is added to additional reports of Russia's suspected cyber intrusions into government entities in Europe as well, and the disruption of election campaigns there.[2] Russia was also suspected of a failed attempt to interfere in the presidential elections in France, with the aim of undermining the election of Emmanuel Macron by publicizing information on the internet that had been stolen from his election headquarters (some of which might have been fake).[3]

Another case of interference in foreign election campaigns is the exposure of people who were behind the rigging of elections in Latin America. Andrés Sepúlveda—who claimed that he led a team of hackers who had spent the last decade trying to rig the results of elections in Latin American countries like Mexico—said that his team had installed spyware in the computers of

[1] Office of Director of National Intelligence, "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution," Intelligence Community Assessment, January 6, 2017.

[2] "Not only in the United States: Russia Interferes with Elections in Europe," *Ynet*, December 10, 2016 (in Hebrew).

[3] Eric Auchard and Felix Bate, "French Candidate Macron Claims Massive Hack as Emails Leaked," *Reuters*, May 6, 2017.

opposition offices, stole election campaign strategies, and manipulated social media to create false waves of enthusiasm or derision.[4]

There is a clear difference between the two cases described above: a world power was apparently behind the first case and attempted to influence the results of the presidential elections in the United States and in France. Private individuals who had been recruited by political rivals were behind the second case.

This article focuses on the first type of threat, that of interference, which we define as "strategic cyber political subversion." This article discusses the vulnerabilities in a democratic country's election process that enable foreign interference and analyzes the components of the process and their vulnerabilities to cyberattacks. This article also presents the elections as a critical process, the disruption of which is liable to undermine a country's democratic stability and the public's faith in democratic institutions altogether.

Between Critical Infrastructure and Vital Cyber Processes

From the American perspective, critical infrastructure is essential systems that constitute the foundation of American society and that support its security, economy, and health systems. This definition relates to sixteen categories of systems and agencies for which the American government is responsible for guaranteeing their physical and cybersecurity. These categories are the chemical industry, which includes the pharmaceutical, agrochemical, and special chemical industries; commercial infrastructure; communications; manufacturing industries, such as the metal industry; energy; dams; security industries for the manufacture and maintenance of war materials and military systems; emergency services; financial infrastructure; the food and agriculture sector; government infrastructure; health systems; information systems; nuclear infrastructure; transportation infrastructure; and the water infrastructure.[5]

In Israel, cyber defense is critical for any public infrastructure, whether under government or private ownership, and that defense encompasses physical protection as well as security of its information and computer

[4] Jordan Robertson, Michael Riley, and Andrew Willis, "How to Hack an Election," *Bloomberg*, March 31, 2016, https://www.bloomberg.com/features/2016-how-to-hack-an-election.

[5] The definition was taken from the website of the US Department of Homeland Security: https://www.dhs.gov/critical-infrastructure-sectors.

systems.[6] Infrastructure is defined as being critical when harm to it is liable to lead to socio-economic damage that could potentially disrupt the state's economic or social stability or its security. For the most part, critical infrastructure has three main characteristics: symbolic importance; the state's functional dependence on them, to the extent that any damage could lead to prolonged impairment and harm to the population or economy; and interactions with other infrastructure.[7] In recent years, additional entities such as internet service providers and part of the financial sector have been added to the traditional definition of critical infrastructure in Israel (electricity, communications, railways, water and fuel lines, aviation, and so forth). A committee chaired by the head of the National Cyber Bureau determines which infrastructure should be defined as critical and it requires legislative amendments. Critical infrastructure must comply with national cyber defense regulations. Regulations are enacted—with input from critical infrastructure entities—by the Information Security Authority in the Israeli Security Agency. A considerable portion of the Information Security Authority's authority is being transferred to the National Cyber Security Authority. Other public services, such as education, health, law, and the election campaigns in Israel, are not defined as critical infrastructure that require direction and guidance from the competent authorities; nevertheless, the Central Elections Committee in Israel receives guidance from the National Cyber Authority.

Demands have been made recently in the United States to update the definition of critical infrastructure and to include additional entities and processes that are vulnerable to cyberattacks, such as election campaigns, research bodies, and academia. These demands are due to the sharp rise in the use of the internet and computerized systems in all sectors (public, business, government, private, infrastructure, and academia), which warrant the reclassification of these infrastructures, given the sensitivity of complex systems that are based on communications and computer infrastructure, including elections systems.[8]

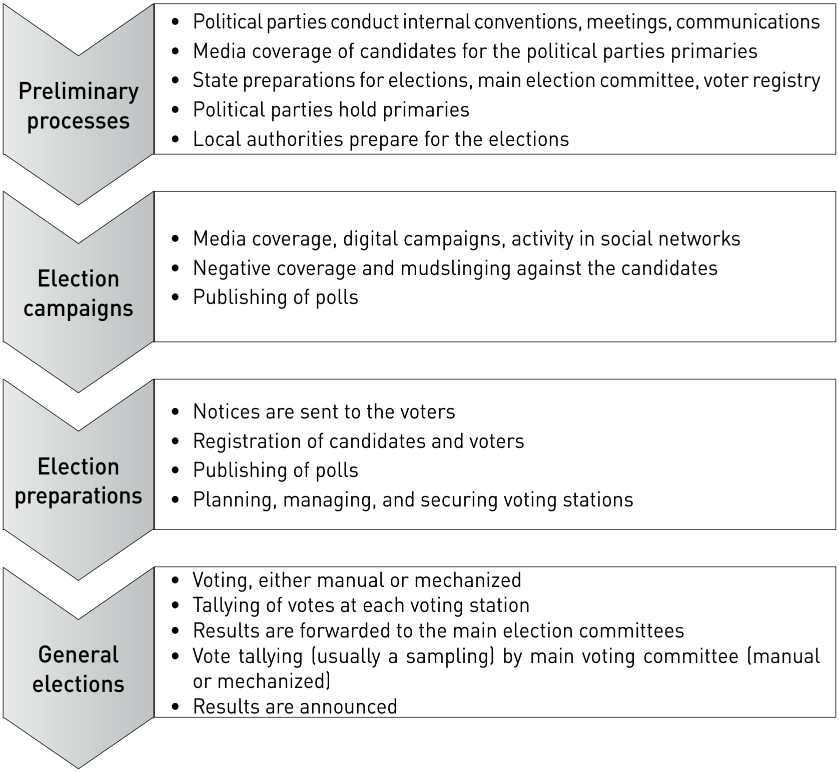
[6] Roy Goldschmidt, "Cyber Space and Defending Critical Infrastructure," *The Knesset, the Research and Information Center, 2013* (in Hebrew).

[7] Lior Tabansky, "Critical Infrastructure Protection Against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (November 2011): 61–78.

[8] Kate O'Keefe and Byron Tau, "U.S. Considers Classifying Election System as 'Critical Infrastructure,'" *Wall Street Journal,* August 3, 2016.

Democratic Election Process – Main Cyber Threats

A democratic election is a process composed of various interacting players and entities. Components of the democratic process increasingly use infrastructure, including cyberspace. The election process is comprised of four stages that proceed in chronological order, as shown in the diagram below. The major cyber threats to this process, against which countries must defend themselves, are attacks on infrastructure, the collection of information about candidates and political parties, and attempts to influence public opinion.



Preliminary processes

- Political parties conduct internal conventions, meetings, communications
- Media coverage of candidates for the political parties primaries
- State preparations for elections, main election committee, voter registry
- Political parties hold primaries
- Local authorities prepare for the elections

Election campaigns

- Media coverage, digital campaigns, activity in social networks
- Negative coverage and mudslinging against the candidates
- Publishing of polls

Election preparations

- Notices are sent to the voters
- Registration of candidates and voters
- Publishing of polls
- Planning, managing, and securing voting stations

General elections

- Voting, either manual or mechanized
- Tallying of votes at each voting station
- Results are forwarded to the main election committees
- Vote tallying (usually a sampling) by main voting committee (manual or mechanized)
- Results are announced

Cyber Weaknesses in the Election Process

Disrupting, altering, and forging of information bases

The government departments that are responsible for recording and saving the personal information of the country's citizens and companies have been undergoing advanced digitization processes and streamlining in recent decades with the installation of computerized systems for registering and managing records. These systems are extremely vulnerable to cyberattacks, as was proven in the US states of Georgia, Illinois, and Arizona.[9] In these three states, cyber intrusions into the e-voting machines were discovered, which could have led to the theft or exposure of the details of about 21 million US citizens. Identity theft and leaking and/or altering voters' details could have ramifications on the entire democratic process.

Exposing a campaign to corrupt citizens' data or causing harm to their voting stations (such as by giving false information about the location of the voting station, potentially disqualifying votes) is liable to adversely affect the public's faith in the election system. One example occurred during the general elections in Canada in 2011, when pranksters telephoned citizens and gave them incorrect information about the location of their voting station, apparently with the aim of diminishing voters' motivation to exercise their right to vote.[10]

In Israel, voters' details are not just saved in the databases of the State and the Elections Committee but are also forwarded to every political party running for election. This situation creates vulnerability in securing voters' information, although, to date, no attempts to disrupt elections in Israel have yet been exposed. This raises the issue of how to guarantee the proper use and supervision of the voters' database in a reliable way.

Hacking of voting systems on election day

Voting during elections, whether by manual or mechanized voting, entails verifying personal details, tallying of the votes at the voting stations, and transferring the data to the main system. Hacking of one of these processes will cause significant harm to the entire process. The electronic systems that facilitate the election day process include various services: registration at a voting station and providing the right to vote; electronic voting at the voting station (either using a touch screen or a personal card); remote electronic voting through internet access only; and tallying the votes. The growing use of electronic voting systems has positive and negative implications: on

[9] Dan Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud," *Ars Technica*, November 7, 2016.

[10] Paul G. Thomas and Lorne R. Gibson, "Comparative Assessment of Central Electoral Agencies," *Elections Canada* (May 2014), http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=p4&lang=e#ftn10.

the one hand, an electronic system should increase citizens' participation in elections (since they can vote from home or from mobile phones); on the other hand, such a system has a higher risk of being hacked and manipulated and requires the investment of resources to secure and maintain it.[11]

A study conducted by the Institute of Cyber Security in the United States, which researches cyber technologies for critical infrastructure, found that the direct-voting system together with the Op Scan system that scans the voting cards; the systems that assess the data; and the computerized databases do not provide terminal-to-terminal encryption or an adequate security solution. It was also discovered that these systems are operated on unprotected computers at many US voting stations, which can be easily hacked. The study also determined that opponents with appropriate capabilities could find a way to manipulate local and political parties' systems, whose level of security is even lower than the state's general election systems, by uploading malware to the computers; disabling the systems; and stealing, exposing or altering information.[12]

Altering the tally of votes

The mode of tallying votes at the close of election day varies from country to country, according to the voting method. In Israel, voting in national elections is done manually, through ballots tallied by hand in the voting stations and input into an electronic system that computes the regional voting percentages to obtain a final national calculation. In 2014, a seminar held in Canada conducted a comparative assessment of the main electoral systems in Britain, Canada, the United States, Australia, New Zealand, and India and reached the conclusion that, in the future, all of the bodies involved in election processes will need to contend with the challenges of the development of network-based systems and their implications on the election campaigns, including securing the on-line or remote voting processes, the databases, and the vote-tallying systems.[13]

Many publications in the United States have discussed the possibilities for influencing the vote-tallying systems and forging the cards that operate

[11] Goodin, "US E-Voting Machines."

[12] James Scott and Drew Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater," *ICIT Blog, Institute for Critical Infrastructure Technology*, October 24, 2016.

[13] Thomas and Gibson, "Comparative Assessment of Central Electoral Agencies."

the electronic direct-voting systems. Thus, for example, an electronic direct-voting system has been introduced in some parts of the United States, identification is verified by using a personal chip card, and voting is conducted on a touch screen. This system saves the data and generates a printout that is produced at the close of election day, which includes the breakdown of votes at each voting station. It became evident that by using a forged card, it was possible to change the data on the screen, alter votes, delete votes, and even remove candidates.[14] Furthermore, despite the identification by card, these systems may be remotely hacked to manipulate the tally of votes and even their segmentation. Electronic voting, which is done via computer with internet access, is even more vulnerable to hacking, fraud, and subversion of the general election process.[15]

Destroying Public Trust by Influencing the Content of the Public Discourse

As stated, besides the election process, there are additional factors that constitute the basis for the public's faith in the country and its institutions. According to one researcher, several characteristics constitute the key components of the public's faith in the political establishments in a democratic country: independent media, active public opinion, an independent judicial system, a fair standard of living (health services, housing, education, and employment), and free elections. Subverting these components is liable to significantly affect people's faith in the country's institutions and public services in general as well as their own personal sense of security in their country.[16]

The emergence of new arenas of discourse and communications in recent years (particularly social media) has led to the development of a wide-scale political and public discourse that addresses a more diverse audience than the traditional media and enables direct contact with citizens and voters. This change has led to the increased use of the internet as an arena for recruiting activists and support, for transmitting messages, and for managing election campaigns. The internet is no longer the domain of marketing and advertising

[14] Goodin, "US E-Voting Machines."

[15] Dimitris A. Gritzalis, *Secure Electronic Voting* (New York: Springer, 2003).

[16] Prof. Marco Meier, lecture, "Cyber, Politics and Elections" conference, Yuval Ne'eman Workshop for Science, Technology and Security, Tel-Aviv University, January 17, 2017.

gurus alone; rather, we have witnessed electoral candidates who have become increasingly active on various media channels, as well as hostile countries that seek to influence public opinion on the social networks and the internet.[17]

Consequently, the protection of democratic processes requires that we add to the direct threats defined above some additional threats that occur in the conscious space, which are liable to critically impact the democratic process and, in turn, the public's confidence in it. In this context, a dilemma arises relating to the need to differentiate between legitimate courses of action in a political battle and illegitimate interference by foreign entities. Defense against such threats does not relate to the direct cyber aspects (defending the terminal stations, servers, networks, and so forth) but rather to interference in the content of the messages within the political discourse. The question raised concerns the limits of free speech: Does it encompass only a country's citizens and leaders or also outside sources—such as foreign countries and terrorist organizations—when their interference is not legitimate and is intended to thwart democratic proceedings? In other words, perhaps we can reconcile ourselves to the phenomena of manipulations, lies, and rumors as a legitimate part of the political battle inside a country, but we cannot accept foreign interference that is liable to undermine the citizens' confidence in their country's institutions, which leads to their destabilization.

The structure of social networks enables content to "go viral" by extensive sharing, which increases its dissemination and its publication based on activity and the reactions that the content generates, and thus magnifies its exposure and publicity. Therefore, it is enough to have a few hundred users (real or fake) who create content targeting a specific audience for the message to "go viral" and awaken a public discourse that the traditional communications media will join. All the above indicates that it is important to examine how we can prevent outside sources from manipulating a country's democratic processes—general elections, processes within political parties, judicial processes, and so forth.

As stated, in recent years, western countries have experienced several attempts to influence the political discourse, which have been attributed to Russia. There are those who believe that attempts to influence and interfere in election campaigns in other countries reflect Russia's intent to undermine

[17] Azi Lev-On and Erez Cohen, *Connected: Politics and Technology in Israel* (Jerusalem: Israel Political Science Association, 2011) (in Hebrew).

citizens' faith in the democratic process in general and in electoral systems in particular, while fabricating a sense that the system is incapable of protecting its citizens' privacy and of ensuring a genuine democratic process.[18] In recent years, it appears that Russia has indeed been doing its best to influence public opinion in countries where it has interests, such as in Ukraine and in the Baltic republics, as well as in Germany, the Netherlands, and France, which represent the most dominant countries in the European Union. Examples of this influence include the cyber intrusion into the Bundestag in Germany in 2015 for collecting intelligence, which would harm the ruling political party, and the attempt to interfere in the referendum in the Netherlands in April 2016, which was held because of a demand to terminate the European Union's 2014 trade agreement with Ukraine. A poll that examined the positions of voters who opposed the agreement found that most of the rationale they gave was false, not based on facts, and apparently had come from Russian propaganda.[19] In addition, there were reports that Russia was trying to influence Britain's exit from the European Union ("Brexit"); the election campaign in the United States in favor of Donald Trump; and unsuccessful attempts to influence the elections in France a few months later.

The examples mentioned above demonstrate the rise in the dissemination of political or strategic information via social networks or websites that specialize in exposing information (such as "WikiLeaks") in order to influence public opinion and public discourse. Entities seeking to influence the discourse and the results of elections can do so by exposing information, whether real or fake, with the right timing. Such exposure is designed to create doubt about a candidate's suitability and to spread rumors that will harm a person's candidacy. These examples also show how elections can be influenced by the spreading of fake news, publicizing false surveys, creating media buzz about a false report that has implications on foreign policy, and leaking of personal and embarrassing information about candidates. All these can influence democratic processes and relations between countries.

The recognition of the growing use of this strategy requires a comprehensive discussion about expanding the defense measures against this threat in

[18] Keir Giles, *Russia's 'New' Tools for Confronting the West*, Research Paper (London: Chatham House, Royal Institute of International Affairs, 2016).

[19] Anne Appelbaum, "The Dutch just Showed the World how Russia Influences Western European Elections," *Washington Post*, April 8, 2016.

democratic countries.[20] Moreover, even if the technological aspects of the election process will be fully protected, it will still be possible to influence the entire democratic process. This is one of the key challenges in defending any election campaign: it is not enough to protect technological infrastructure and systems; a defense response is also needed for the entire discourse against outside anti-democratic corruption. If, in the past, the attacker had sought to disrupt communications and computer systems, now, in the era of the new threat, the attacker is actually interested in ensuring that these systems continue to operate so that the attacker can inundate them with manipulative messages.

Factors Threatening the Democratic Election Process

The cyber threat to election campaigns can be expressed by the interference of world powers or foreign countries, international criminal or terrorist activities. The types of threats are differentiated by identifying the attacker, the motivation for the attack, its sophistication and complexity, and the available resources for executing the attack. In order to protect the election proceedings or any other critical infrastructure, risk management needs to include an analysis of those players who are motivated and able to subvert the democratic election process.[21] An article that analyzed the sensitivity of the election process following the Russian attempts at interference, examined, inter alia, which of the various players could carry out a cyberattack against components of the US election system. Included among them were hostile countries, internal rivals, and individual hackers, the latter acting out of ideological motives, such as members of "Anonymous" or "WikiLeaks," or funded organizations with political ideologies that work to influence the elections through massive campaigns on social networks and among young people.[22]

[20] "Emerging Cyber Threats to the United States," Testimony of Frank J. Cilluffo, director of the Center for Cyber and Homeland Security before the US House of Representatives' Committee on Homeland Security, and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, February 25, 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf.

[21] Goldschmidt, "Cybernetic Space and Defense of Critical Infrastructure."

[22] Scott and Spaniel, "The Painfully Vulnerable Election System."

The motives of rival countries for interfering in the election campaigns of another country vary according to the target of the attack. One motive can be the desire to undermine the public's sense of personal security and faith in the entire democratic process. The understanding that public opinion has an impact on how policies are set motivates rival countries to incite citizens against the democratic framework and, mainly, against the government and the politics within the country. Another motive for interfering in another country's election campaign is the desire to influence the outcome of the elections. Therefore, the interfering forces will invest their resources in several channels: influencing public opinion through propaganda, for example, by planting "trolls" who operate throughout the internet against the establishment and sometimes against the internet community; disseminating negative and inflammatory reactions to particular information; hacking of websites; spamming; subverting public opinion and faith in the system; and leaking sensitive information about rival candidates. Another motive may also be to engage in espionage and intelligence collection, including the theft of sensitive information about the candidates or about their election headquarters, as was done during the summer of 2016, when e-mails were leaked from the Democratic Party's convention.

Conclusions

This article presents the threats to election campaigns, as well as the cyber and cultural developments and underlines the importance of recognizing election campaigns as critical infrastructure and processes. The conclusion is that an overall defense of the election process is needed because its external influence is liable to completely undermine the public's faith in the political establishment in their country and democratic values altogether. Leaders in Israel's national cyber organization have demonstrated their understanding of the importance of defending the computer systems of the Central Elections Committee and the database of voters, and they agree that a legislative amendment may be necessary to define these systems as critical infrastructure; however, it appears that the need to protect the political discourse from external interference is still not yet understood.

An election campaign is a "soft spot" in a democratic country, and an attack on it is liable to influence both the country and the candidates. Western countries should consider expanding their approach and the modes of response to threats to the democratic proceedings, such as by safeguarding the media discourse and defending political parties, coupled with protecting election committees and voting mechanisms. Defending only one component of the overall system will not be enough, however. The attempts to influence elections by exposing and publicizing information stored in the computer systems of political parties or candidates, some of which have apparently succeeded, demonstrate that the defense of these systems must be enhanced. Those attempts also give rise to the question about the country's responsibility to lead the cyber defense of political institutions.

This article does not discuss responses to threats facing the election system in democratic countries, as it intends at this initial stage to enable a discussion about these threats, particularly those endangering the political discourse in democratic countries. Directing the spotlight on external threats emphasizes the role that a country's security establishment has in thwarting threats of political subversion. This also requires the security establishment to define the threats and to delineate them in a way that will protect freedom of expression on one hand and will also protect the political discourse from illegitimate interference on the other.

The challenge of defending the election process and all other democratic processes, such as the rule of law and freedom of expression, is not just safeguarding the operation of the infrastructure; rather, it also encompasses the preservation of the public's faith in the system, which is a far more evasive achievement that may be undermined in a variety of different ways. Thus, this article presents the need—for which there is wide consensus—to defend the network of computers that operates the election system. In addition, it addresses the necessity of protecting the political discourse from external interference, which seeks to undermine the public's faith in the entire democratic system but is still not widely recognized, because, inter alia, it challenges the democratic principles, such as safeguarding freedom of speech (in social media and the traditional media).

“The Missing Effort:” Integrating the “Non-lethal” Dimension in the Israeli Military Lines of Operation

David Siman-Tov and David Sternberg

This essay examines the idea of “Non-lethal warfare” and how it can and should be integrated in the framework of the IDF’s military campaigns. It addresses the organizational, conceptual, and cultural barriers obstructing such a policy, and the changes required in the IDF’s operating principles: establishing the guidelines; changing the concept of time in a military operational design; shifting from a structure of covert to overt campaigns that are connected to the civilian environment; and devising a supportive intelligence and operational mechanism. In practical terms, the way to promote “Non-lethal warfare” in the IDF requires focusing on four relative advantages: technological innovation; Israel’s relationship with the United States and other strategic partners; utilization of the compact size of the defense establishment; and reliance on acquiring civilian know-how through the reserve system, or creating other mechanisms enabling know-how and “soft” capabilities acquirement.

Keywords: Soft power, Non-lethal warfare, Non-Kinetic warfare, Influence operations, Information operations, situational awareness, IDF strategy, lawfare, economic warfare, psychological warfare

David Siman-Tov is a researcher at the Institute of National Security Studies. David Sternberg is a graduate of the Harvard Kennedy School in public policy.

Introduction

In his book, *The Utility of Force*, British general Rupert Smith stated that the change in the current battlefield has turned "warfare between peoples" into "warfare amongst the people."[1] What he meant was that in the modern world, in which communications, public opinion, and global considerations are of growing importance, concepts such as "decisive victory" are obscure and dependent upon how relevant audiences—who are not necessarily a direct part of the military campaign—perceive and recognize them. This contrasts with classical warfare, in which the victor alone is the one that determines victory on the battlefield.

In the background of this change are two overriding trends that characterize the modern global environment. The first is the information revolution, which has increased the speed of change of information, its accessibility, and patterns of its consumption, and moreover, transcends borders and sovereignty. In this framework, conceptual connectivity and technological networking enhance an individual's capability; at the same time, they augment the systematic vulnerability of nations and societies. The second trend includes the changes that have occurred in the political-diplomatic field. Over the past two decades, we have witnessed a growing significance of non-governmental organizations; greater consideration of public opinion in making security decisions; the emergence of international quasi-legal agencies; the growing influence of lawfare; and a lively discourse on human rights as a major criterion in considering the legitimacy and legality of using military force.

Two central arguments can be derived from these changes. First, nations face difficulty in controlling information and shaping the narrative and legitimacy of their actions. Second, the effectiveness of lethal or kinetic force lines of efforts for achieving strategic objectives has been weakened. In addition, the use of lethal force has exacted political prices from state armies in numerous cases, so that many prefer not to use it. Given these changes, and the wish to develop means of exerting ideological, cultural, and economic influence instead of solely military might, the "soft power" approach emerged as a basis for the defense and foreign policy for major Western powers and many countries. The concept of "soft power" refers to

[1] Rupert Smith, *The Utility of Force – The Art of War in the Modern World* (London: Penguin Books, 2005).

the ability to persuade others to act in accordance with one's wishes without using physical force but rather by non-lethal resources and capabilities, such as economic, legal, diplomatic, cultural, and ideological resources.[2]

The problem with soft power is its need to cope with changes in the enemy's DNA as well as in the environment. In current conflicts, an imbalance exists between the traditional state armies and the new players with which they must confront. While the traditional state armies are characterized by bureaucratic inflexibility—both conceptually and resourcefully—the new players embody elements of flexibility, innovation, and the ability to adapt. These features enable the new players to make optimal use of the new strategic field. This dichotomy between the two is not a decree of fate, and some state armies have shown a strong desire to adapt and acquire operating capability in the use of non-lethal tools, which we will refer to in this article as "soft" tools.

This essay examines the idea of non-kinetic warfare and how it can and should be integrated in the framework of Israel's military campaigns. The first section in the article is theoretical; it surveys the source of the concept and its elements and cites some examples of parties that have adopted "soft" reasoning as a key part of their operational strategy. The second section presents the Israeli perspective about the need to adopt the logic of influence operations. The third section analyzes the challenges and obstacles of assimilating "non-lethal" logic in the IDF's operational concept. The final section presents the principles of the response to these challenges and recommendation for future directions of action.

It should be noted that "non-lethal" efforts are not confined to the army alone; other governmental agencies in Israel need to use them—and some already do—as part of Israel's security and foreign policy approach, among other things, to facilitate the IDF's actions. This essay does not address the entire national effort, although the army needs to develop close reciprocal relations in order to realize the joint potential of the security, government, and private sector so that Israel's interests can be promoted.

Theoretical Background

The root of "soft" action lies in the recognized historical arsenal of political and strategic concepts and tools. However, the profound, changing character of the new conflicts and challenges for armies that developed in the modern

[2] Joseph Nye, "Soft Power," *Foreign Policy*, no. 80 (1990): 153–171.

era leads to more intense efforts to develop soft tools. For example, it is not easy to attack terror and guerilla organizations embedded among a civilian population because of the intelligence and operational difficulties as well as the fear of harming uninvolved civilians, which is liable to lead to a Pyrrhic victory and a loss of legitimacy. Another example is the development of weapons and their transfer to terrorist and semi-military organizations, often occurring between wars; dealing with them involves the use of political or economic pressure. A final case comes from the realm of cyberwarfare; the target is not necessarily destroying an infrastructure (the enemy's weapons systems) but rather causing effects at a higher level of cyberspace in the cognitive-semantic level, including effects such as deception, confusion, paralysis, embarrassment, and so forth. To influence this realm, new planning and action tools are needed.[3]

The sources for military thought about non-lethal warfare have been deeply rooted in security and military endeavors for many decades. For example, the United States has a considerable history of Train and Equip strategies as well as psychological and economic warfare operations. At the national level, the American soft power paradigm, which was conceptualized in the 1970s as part of the cold war era, kept its prominence also in the last decade in the form of the "smart power" strategy of the Obama administration, as employed by the imposition of effective financial sanctions against Iran and Russia as well as actions in the cybersphere. Recognizing the military potential, the United States military has in recent years established a special command for cyberspace and has strengthened the role and organization of information operations (IO).[4] Even if the ability to judge the effectiveness of this activity is limited, it is clear, nevertheless, that it is being planned and integrated into US military efforts. Furthermore, soft warfare is expected to gain in importance and expand greatly in the coming years.[5]

As initially defined, the concept of "soft power" referred to the ability to persuade others to accede to one's wishes without the use of physical power against them. The original intention underlying the concept was to disseminate liberal democratic ideas and concepts using cultural and

[3] M.C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007).

[4] Joint Chiefs of Staff, "Information Operations," Joint Publication, 3–13, 2016.

[5] DCDC, "The DCDC Global Strategic Trends Program, 2007–2036," http://www.cuttingthroughthematrix.com/articles/strat_trends_23jan07.pdf.

economic tools (along the lines of Thomas Friedman's "Golden Arches" theory, which argued that globalization would prevent violence between countries).[6] To this day, this original purpose is best reflected in the way that the rivals of the United States perceive the main threat that soft power poses to their stability. For example, Russia, China, and Iran all fear mostly the economic, media, and cultural abilities of Washington to "fuel" internal forces in their countries and bring about a "velvet revolution."

A recent RAND Corporation study produced for the US army concluded that the traditional dichotomy between "soft" and "hard" requires refinement and clarification. The study proposes an intermediate conceptualization between the use of military forces and soft forces based on positive diplomacy with a long-term vision. The study calls this new sphere the "power to coerce" (P2C). It includes a broad range of measures, such as economic sanctions, military assistance to opposition forces, cybernetic offensive warfare, psychological warfare, and more.[7]

These concepts are dominant in the cultural and philosophic practices and military doctrines of other countries as well, including Russia and China. In the case of Russia, "hybrid warfare"—as it is referred to in the West—has been manifested in several theaters, e.g., the invasion of the Crimean Peninsula, the broader conflict with Ukraine, and the Russian military intervention in Syria. The subject of extensive discussion in defense and academic circles, one of its prominent features is the combined use of military force with political subversion, economic coercion, and awareness campaigns. Cyber operations are also prominent in this framework (such as in Georgia, Estonia, Ukraine, and possibly recently in the United States), as is the use of proxy forces and agents (for example, the infiltration of forces for guerilla operations in Ukraine), disinformation attacks, and extensive propaganda (for example in Georgia and Ukraine).

The emphasis on these forms of action has been apparent in the war waged by Russia in Syria. These measures include sustained actions, such as sowing confusion about the purposes of Russia's involvement, for example, by declaring warfare against terrorism or "withdrawal" or "the termination of

[6] Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus, and Giroux, 1999).

[7] David Gompert and Hans Binnendijk, "The Power to Coerce" (Santa Monica: RAND Corporation, 2016).

fighting" in order to give the appearance of international legitimacy through channels of dialogue with the United States and humanitarian ceasefires; the use of irregular forces (through Iran and Hezbollah); projecting an image of power in a series of well-publicized actions, including launching bombers and cruise missiles from Russian territory; naval maneuvers; the deployment of long-range air defense systems; and presenting disinformation about achievements.

Even though it is disputable if this is a new model,[8] the cultural and military basis supporting this possibility should not be ignored. This includes for example fundamental concepts such as "reflexive control," which assigns a major role to military actions in creating provocative measures aimed at producing planned responses from the enemy and channeling them into spaces that the strategic planner is trying to reach.[9] Russian chief of staff, Valery Gerasimov,[10] in an article in 2013 made explicit statements about the Russian warfare doctrine and alluded to possible explanations, such as turning to non-kinetical methods in order to compensate for Russia's weakness in the lethal arsenal and limited long-term endurance. In addition, over the past decade, Russia has learned from the West about the significance of the use of soft power and acquired experience in its own conflicts, such as in Estonia. All of this suggests a major conceptual and actual change in the Russian doctrine of warfare.

The integration of soft power can also be seen in the Chinese strategy of "Three Warfares." This strategy holds that it is necessary to combine three types of warfare—public opinion warfare, psychological warfare, and legal warfare—to achieve strategic objectives. The Chinese chief of staff published an official guide on this subject as early as 2005, and important Chinese military writings in recent years have indicated that the strategy is being applied. These publications indicate that the "Three Warfares" strategy is designed for use in both peacetime and wartime and has multiple purposes,

[8] Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's Hybrid War," *Kennan Cable Wilson Center,* no. 7 (April 2015).

[9] Dima Adamsky, "Cybernetic Operational Art: From the View of Strategic Studies and From a Comparative Perspective," *Eshtonot* (Israel National Defense College), no. 11 (August 2015).

[10] Max Fisher, "In D.N.C. Hack, Echoes of Russia's New Approach to Power," *New York Times*, July 2016, https://www.nytimes.com/2016/07/26/world/europe/russia-dnc-putin-strategy.html?_r=0.

including controlling public opinion; implementing strategic communications; undermining the enemy's determination; creating division among the enemy; and imposing legal restrictions. This line of action is evident in the dispute with the Philippines in the South China Sea, where the Chinese utilized a system of diplomatic, legal, and propaganda tools in their struggle to legitimize their control of territorial assets involved in the conflict.[11]

Armies in the Middle East are also applying this strategy. A statement by Iran in 2013 hinted to the establishment of a "soft warfare" headquarters—which will affect the structure of the General Staff of the Iranian army—in recognition that the virtual sphere is a "an important, complex, and convenient weapon of the enemy."[12] The Iranian preparations for soft warfare, as indicated by this announcement, is defensive as it is a reaction to Western power; it indicates, however, organizational deployment in this new sphere, which may also include offense derivatives.

Thus, given the increasing changes in the strategic environment in recent years, the strategic and operational discourse reveals a new definition of soft warfare that uses familiar tools but with new force, diversity, and sophistication. It emphasizes the information revolution and cyberspace, economic objectives, and information campaigns. According to the new approach, a successful non-lethal warfare effort combines overt and covert means. It leverages intelligence superiority and a profound knowledge of the adversary to focus secondary efforts in shaping knowledge and public opinion and disrupting and influencing decision making, all combined with traditional kinetic military measures.

The Israeli Angle

Israeli military history is replete with scars from attempts to exert influence operations, such as in Operation Peace for Galilee in 1982 and the complex relationship with the Christian factions in Lebanon and later during the Security Zone period with the South Lebanese Army. Declarations by leaders of the Israel Defense Forces (IDF) at the beginning of the Second Intifada about an Israeli victory seared into Palestinian consciousness so that

[11] Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief* (Jamestown Foundation), 16, no. 13 (August 22, 2016): 10–14.

[12] Tal Pavel, "Iran Establishing Regional Headquarters for 'Soft Warfare,'" Middleeasternnet.com, October 26, 2013 (in Hebrew), https://goo.gl/wAhg4r.

they would believe that they were losing the conflict; As well as measures designed to shape knowledge in the Second Lebanon War (such as hoisting the Israel flag in Bint Jbeil) have generated skepticism in the IDF's ranks toward such approaches.

Nonetheless, in the past decade, Israel and the IDF have experienced a series of significant events that have raised again the need to harness these capabilities in the military. These events highlighted the price paid for neglecting the non-lethal dimension, in contrast to the adversary's extensive use of it, such as the Mavi Marmara flotilla to the Gaza Strip, Operation Cast Lead, and Operation Protective Edge. At the same time, other events have revealed the benefits that these tools can provide such as the successful diplomatic campaign against Iran.

Israel is faced with a series of unique challenges that require non-lethal operational tools. First, the IDF is one of the few Western armies that is obligated to significantly maneuver in difficult urban, highly populated environments against asymmetric enemies. In addition, at the same time, the IDF has to deal with the ongoing threats of attack on the home front and strategic infrastructure and the adversary efforts to offset its strategic advantages, by operational "surprises" such as utilizing the underground warfare to penetrate its lines of defense. This translates into substantial difficulties in presenting victories in kinetic terms, especially when an adversary exploits and leverages unintentional peripheral damage in order to increase the pressure on Israel's political and operational freedom of action and to offset its achievements.

Second, Israel lacks the resources for supporting large-scale military campaigns due to the amplitude of the geographical arenas and the type of challenges with which Israel must cope. In this case, non-kinetic tools can help to enhance physical achievements, employ deceptive measures for destroying the enemy's resources or to create a surprise that will facilitate fulfilling the operational plans, to form appealing operational alternatives.

Third, since Israel faces both emergent risks and dangers far beyond its borders the non-kinetic tools can serve as an alternative to address issues of prevention and design. This involves, for example, using political and economic means to reduce the proliferation and development of weapons before they reach the battlefield, or alternatively, designing the conditions of the campaign by shaping the attitudes of a population in certain areas toward Israel.

As mentioned above, the concept of soft power is shaped by the experience, conditions, and capabilities of the major powers, such as by employing sanctions, by moving military forces in order to signal intentions, and by massive use of communications tools. Countries like Israel are also capable of adopting a hybrid model, involving the use of more focused tools, such as media, electronic warfare, financial or cybernetic campaigns to enhance the military component and create optimal conditions for its use.

In the military discourse, this mode of action has already been recognized in the space of military action that is "under the threshold." The "IDF Strategy" from 2015 also defines the problem of the enemy's operations "in non-military-kinetic dimensions . . . from within population spaces, or in the underground, media space" that in his eyes, are "successful in thereby offsetting Israel's achievements in the campaign." The document holds that the solution to this problem lies in a "multidimensional approach during and between campaigns, which includes cyberattacks and a conscious-raising and legal effort."[13]

The academic discourse in Israel has also asserted that traditional military efforts are inadequate and that Israel should develop a multidisciplinary approach that integrates political, media, economic, legal, and cyber components, as well as humanitarian aid to its allies as part of Israel's regional strategy.[14] This is a direct continuation of the distinctions made at the Herzliya Forum in 2010, which called upon giving high priority to the threat of soft warfare and to prepare for it by establishing state agencies specifically for this task. Although the document produced by the Forum discusses only defensive aspects that Israel should adopt vis-à-vis soft warfare (political or legal) that is used against it, it now seems appropriate to consider adopting offensive logic as well. The recommendations calling for changes in the political, legal and media spheres are valid for both

[13] Chief of Staff's Bureau, "The IDF Strategy," 2015, p. 12.

[14] Udi Dekel and Omer Einav, "Revising the National Security Concept—The Need for a Strategy of Multidisciplinary Impact," *INSS Insight*, no. 733 (August 16, 2015).

offensive and defensive aspects, and to emphasize intelligence deployment in support of these efforts.[15]

Challenges to Incorporating Soft Warfare in the IDF's Operating Concept and Operational Planning

Understanding strategy is not enough to bring about an operative change in IDF practice. Such a change requires clarification and development among those concerned with the depth of military practice and the translation of soft principles into operational, organizational, and professional practices; several significant barriers, however, stand in the way of integrating the soft logic and tools into IDF thinking in general, and into the operative plans specifically.

The first set of obstacles involves conceptual and organizational matters, beginning with the dividing line between non-lethal operations and the kinetic effort. The operational commander, who usually is inexperienced in matters unrelated to the use of military force, finds it difficult to integrate soft warfare logic into his operational plans, especially when, in most cases, the achievement sought and the criteria for evaluating the success are not clearly defined. The perception of the importance of non-lethal measures in the decision-making equation is thus distorted. A kinetic operation (for example, a targeted killing or destroying a tunnel) will usually be considered more significant and attractive than a soft action, the effect of which is more difficult to assess. This means that in most cases, commanders will not be willing to devote their attention to a non-kinetic operation, allocate data collection resources, risk the exposure of sensitive information, invest time nor prefer the risk that a non-kinetic operation incurs over a kinetic one.

Furthermore, since many of the soft spheres are the fields of disciplinary experts, another organizational bias is created. As long as non-military disciplines are involved, the default option will be to place the non-kinetic planning in the hands of professional parties as a side effort. The spokesperson, military lawyer, liaison officer, intelligence officer, and psychological warfare personnel constitute a "black box," of secondary importance to the operational thinking led by the commander. Furthermore, the professional agencies that

[15] Shmuel Bar, Shmuel Bachar, and Rachel Machtiger, "The Soft Warfare against Israel: Motives and Solution Levers" (Working Paper for the Herzliya Conference, 2010), (in Hebrew), http://www.herzliyaconference.org/_Uploads/3036HateHeb.pdf.

deal with these elements are naturally less willing to concede their professional monopoly by creating an organizational whole that seemingly detracts from their status. Finally, the conceptual-organizational matter is burdened by the absence of a natural habitat in the army for content personnel in the non-kinetic spheres. As a result, the thinking, experience, and modus operandi—which have become more sophisticated in the civilian environment—have grown isolated, weak, and anachronistic in the military incubator.

The second and more significant set of obstacles concerns the Israeli military culture and the ethos of the IDF.[16] This culture values first and foremost action over words and concrete results and achievements over tiresome processes, and therefore its time horizon is usually short. Evidence of this can be found in the dubious dialectic that the IDF has been conducting for a decade or longer with the school of systematic thinking concerning the existence or non-existence of "intellectualism" in the military system and its importance.[17] From here, it is only natural that the basic military culture objects to any investment in overt elements, propaganda, public acts, and operations whose contribution and success is difficult to assess. In Israeli strategic culture, promoting a deeper and more comprehensive measure—which is not only in the form of special units or an investment in concentrated efforts but rather a total integrated effort—requires a deep sense of crisis.

Directions for Future Thinking in the IDF

The necessary changes in the operational principles of the IDF should be implemented in three dimensions. First, the army's operating theaters requires the development of new non-lethal lines of action as part of the basic military capability. Second, the time dimension of military action should no longer distinguish between war and getting ready for war; rather war begins before the campaign, and continues after it. Third, the structure of the military system requires a structure of action that moves from covert, hierarchical, and homogeneous systems to overt and networked systems that communicate with the civilian environment.

[16] Dina Adamsky, *The Culture of Military Innovation* (Stanford: Stanford University Press, 2010).

[17] David Kimhi, "The Intellectual Revolution in the IDF," *Ma'arakhot,* no. 464 (December 2015): 14–25, (in Hebrew).

The way forward is to devise an operational concept that focuses on the four relative advantages of the IDF and Israel: technological innovation; the ability to rely on the special relationship with the United States and other like-minded partners; the compact size and thus agile character of the defense establishment, intelligence community, and governing system; and the acquisition of civilian know-how through the IDF reserves system and through the development of flexible methods of communications with relevant parties in the civilian sector.

The Operating Theaters—From Kinetic to Non-Kinetic

The communications, diplomatic, economic, and legal activity includes a broad circle of partners in the national and international arena. In the case of Israel, this community includes various government ministries, the intelligence community, public relations apparatuses, and private parties. These partners possess the professional knowledge, experience, and network of connections needed to propel action. They also operate in international spheres vis-à-vis state agencies, international organizations, civil society, media and economic institutions and mechanisms, and so forth. With these parties, the IDF's unique role in the context of developing knowledge and operative non-lethal tools is questioned.

The IDF has two main strengths beyond the military and security aspects. The IDF can be an important source of data, information, and knowledge necessary for the existence of any soft power system. Above all, this is due to its being a key target of the adversary (for example, to undermine the legitimacy, freedom of action, and image of Israel in the world) and secondly as a major initiator of events in all the theaters of conflict. The IDF has many strong and relevant operational arms, such as intelligence, the military liaison, media, and legal branches. These mechanisms, its resources, and human capital are likely to provide a basis for operation on a nationwide scale. At the same time, it should be noted that in the non-kinetic spheres of action, a leading role is played by civilian parties—government and private—and the IDF must connect with them in various creative ways.

In order to promote its capabilities in the soft power field, the IDF should therefore create new capabilities or enhance its existing ones in the following areas:

1. *Information warfare*—This type of warfare utilizes the overt, covert, and international media sphere to deliver messages designed to influence large target audiences, including the adversary's audiences, the regional theater, the international theater, and the internal theater. These messages have various purposes, including deterrence, weakening the enemy, deception, counter incitement, and so forth. Such warfare can be focused on a specific person, an organization, social groups, population groups, and audiences.
2. *Political-legal warfare*—This type of warfare relies on the international diplomatic system. It is utilized in frameworks of diplomatic, military and legal cooperation as well as in the international, public, and clandestine spheres. Lawfare can be a defensive means for coping with legal claims against Israel, but it should also engage in potential offensive efforts, such as suing parties acting against Israel or lobbying international institutions.[18]
3. *Economic warfare*—This type of warfare relies on damaging the adversary's financial resources and assets in order to weaken its buildup of force, operational capability, and willingness to continue taking action. Israel and other countries have taken well-known and diverse actions against recalcitrant countries (Iran, Syria, North Korea, and others) in recent years as well as against various terrorist organizations.
4. *Cyberwarfare*—This warfare utilizes cyberspace for achieving various purposes: kinetic, informational, intelligence gathering, and so forth. Cyberspace contains opportunities for influence warfare and can be integrated into other spheres, such as media or economics or be used alone. Examples of soft cyberwarfare include: disabling the network of a country or organization; exposing and publishing sensitive data; disrupting central processes in a country in order to create disorder, and so forth (for the purpose of this discussion, cyberattacks against weapons and infrastructure are not included in this article).

Time of the Operation—From a Sprint to a Long-Term Effort

The concept of time also requires change. Military endeavor should shift away from its division into two classic fundamental situations— "war" and

[18] Noam Neuman, "Lawfare—Threats and Opportunities," *Ma'arakhot*, no. 449 (June 2013): 22 (in Hebrew).

"preparing for war"—to a broader and more complex perspective of the dimension of time, which should include the following:[19]

1. *The continuous effort* includes the actions taken in peacetime aimed at preventing a conflict. This effort is designed for purposes such as deterrence, slowing escalation processes, creating and leveraging influence, and enhancing assets or changing a problematic situation.
2. *The conflict-shaping effort* is also conducted in peacetime. It is aimed at predicting the nature of future conflicts, creating the optimal conditions for victory, and designing the future battlefield. One example of this is promoting international understanding for the possible need of using certain armaments or forms of warfare essential to IDF maneuvering.
3. *The preliminary effort* is directed at maximizing the conditions for victory in a campaign as they appear in the existing operational plan. For example, this can include operational deception devised over time that weakens the adversary's concept of a specific capability or operational intention of the IDF.
4. *The delayed accompanying effort* includes the operations accompanying the campaign and its results. As soon as the campaign begins, the operational plans change. The enemy's response creates a new situation that requires renewed planning, reveals new facts, and leads to unforeseen results. A capability to respond is therefore also needed. Examples of such responses is influencing the enemy's perception of its achievements, assistance in designing effective end mechanisms, and softening negative influences on the IDF's future freedom of action. In addition, after the war, political and legal issues will arise, for which more legal and other soft efforts will be needed for response.

The Structure of the Campaign and its Relation to the Environment: From Covert to Overt

The preparation required to employ non-lethal efforts in the military endeavor is a challenge for the IDF, which has been oriented toward lethal actions and has limited its non-kinetic efforts to the media activity of the IDF spokesman, focusing mainly on the Israeli public. As noted, the IDF has not given rise to soft efforts, because the people who have been educated in these spheres and

[19] Gur Laish, "Principles of the National Security Council's Defense Concept," *Eshtonot* (Israel National Defense College), no. 10 (July 2015): 41 (in Hebrew).

who engage in it are not the typical army officers. The obvious conclusion is that the structure of the action in the soft dimensions must be overt and flat, and should not take place between the ends of the bureaucratic pyramids but rather should occur in a joint area.

For producing substantial joint efforts, the IDF will need a different model of action. Such a model will have to create a network of daily action in the military circle, in which the ability to integrate the relevant command headquarters and action groups is necessary; and among the state authorities through coordination, synchronization, and harnessing of important partners in the government ministries and other authorities. Finally, unlike the IDF's secretive instincts, a structure is needed that will promote cooperation, dialogue, and harnessing of partners, such as research institutes, non-profit organizations, service providers, key countries, parties at the UN, civilian organizations, and NGOs.[20] This network would provide the army and its partners with two important "bridges." The first is the ability to extract relevant information from the security arena in order to initiate, plan, and promote exposure and influence activities through open platforms. The second leads to an understanding of the civilian theater, the opportunities and risks inherent in it, and the professional capabilities and experience acquired by those involved, all for designing an optimal military action.

Principles for Designing a Non-Lethal Concept in the IDF

Israel has four main advantages that should be leveraged as part of promoting a non-lethal warfare concept in the IDF:

1. *Highly developed technological capabilities*, especially in information technology and social networks. In this sphere, with all its complexity, Israel's special quality and natural innovation should enable it to develop new lines of effort to support its military activities. A comparison can be made with the global reputation that some Israeli army units acquired, such as Unit 8200, in the field of intelligence collection that could be paralleled to an appropriate response in the world of influence.[21] Furthermore, the increasingly powerful medium of social networks is

[20] "The Delegitimization Challenge—Creating a Political Firewall," Reut Institute, January 2010 (in Hebrew).

[21] Zvi Hauser, "Redefining Israel's National Security," *Ynet*, April 5, 2016.

generating possibilities and ways of influence that did not previously exist and that represents great potential for action.

2. *The special relationship with the United States*. Israel's relationship with the United States should enable Israel to exercise indirect influence on its military campaigns and on the international environment through cooperative influence efforts and the combination of complementary capabilities.
3. *The advantages of compact size*. One important advantage of the Israeli defense establishment is its ability to integrate between different national agencies easily and rapidly. While cultural, political, and technical difficulties also make this task challenging, it appears that the IDF's dominant weight, combined with its relative agility and flexibility, can render it more productive in activating non-lethal warfare than its counterparts. For example, creating an organizational connection between the parties (not necessarily creating one agency) and creating a concept of joint action between all the agencies in the IDF or the Israeli intelligence community can constitute a force multiplier for advancing the subject. Promoting comprehensive training in the IDF can also lead to a systemic change in the army's awareness of the importance of the issue and in its integration into operational thinking.
4. *Integration with the civilian sphere*—Given that the army has access to most of the civilian content experts through the reserve system, there is a better chance of successfully connecting the civilian professional know-how and military knowledge through this informal network. In addition, it is necessary to develop new tracks to connect between the security sector and the private civilian one, which will better utilize the civilian knowledge in the military endeavors, and will enrich military knowledge with ideas, tools, and methods of action developed in the civilian and governmental sector.

Nonetheless, effective systematic operation using non-kinetic tools requires two basic conditions**.** The first is an **operational concept**. The non-lethal effort should be connected to the operational idea. Such an effort cannot come at a later stage, because it is mostly derived from the strategic aspects related to the narrative of the military action, its mechanisms of termination, national resources, and an understanding of the enemy's intentions and capabilities at the overall level. The second is a **supportive and empowering intelligence**.

Carrying out influence operations requires the development of a new type of supportive intelligence that builds a systematic understanding of the new goals and issues: social, cultural, economic, media, organizational, and personal. It also requires the allocation of some of the Military Intelligence operational capabilities. In addition, there is a need for developing an approach and mechanisms that will facilitate rapid publication and operational use of information and knowledge; intelligence organizations, which operate covertly and preserve their sources, are naturally not inclined to publish them.

Conclusion

This essay examined the idea of soft warfare from a theoretical, military, and strategic perspective, and how it is expressed in the strategic and operational endeavor of the major powers in the information and cyber era. The Israeli angle and the unique challenges faced by the IDF were assessed in this context, including ways that soft efforts can and should be integrated into the framework of Israel's military campaigns.

At the same time, the organizational, conceptual, and cultural obstacles to adopting a soft approach in the IDF's strategy and its operational concept were assessed, and the main changes needed in the principles of the IDF's operation for enhancing the non-lethal dimension were presented. In this framework, the article emphasized the establishment of methods and tools that should be utilized in combination with lethal efforts, the change of the concept of time of the military operation, the move from covert to overt systems that are connected to the civilian environment, and the building of a supportive intelligence and operational mechanism. In practical terms, the way to promote the non-lethal dimension in the IDF requires a focus on the four relative advantages that the IDF and Israel enjoy: technological innovation, the relationship with the United States, the compact size of the defense establishment, and reliance on acquiring civilian know-how through the IDF reserves system or by creating other mechanisms for the flow of information and soft capabilities.

Not Merely a Technological Advantage: The United States' Organizational Change in Cyber Warfare

Amit Sheniak

The cyber arms race is part of the state security reality in our times, resulting in a sharp increase in the allocation of resources for the technological development of new defensive and offensive cyber capabilities. This article stresses that a different policy should be taken, arguing that due to the unique characteristics of the cyber dimension and the declining level of technological sophistication needed for offensive and defensive cyber capabilities, a security advantage in this field will results from a creative advancement and development in force organization specifically by formulating a new doctrine of warfare, which will aim to improve the integration of security activities in both cyberspace and in physical spaces. The review stresses the changes and increased scale of cyber threats, the changing perception of the threat, and the transition from a technical approach to one that regards the internet as a new operational space with unique characteristics. This article is based on a comprehensive review of the legislation, plans, and decisions concerning the force building organizational process, and cyber operations doctrine in the United States from the early 1980s through 2012. Although the article focuses on the United States during a limited timeframe, its aim is to shed light on the field of organization as a relevant and significant theater in which a political advantage in cybersecurity can be achieved, in contrast to the current state in which researchers and decision makers focus

Dr. Amit Sheniak is a post-doctoral research fellow in the Science, Technology, and Society (STS) study program at the Harvard Kennedy School of Public Administration.

more on technological development as the tool for acquiring an advantage in this sphere. The conclusions of the article are relevant to both professionals and decision makers.

Keywords: Cyberspace, cyber security, force building, organization, theory of warfare, United States, strategic advantage, dominance

Introduction

The struggle between countries in the cyber realm has been evident for quite some time and has been a frequent subject of research in the fields of security studies and international relations.[1] The arms race and military force building in the cyber realm have been manifested by a significant increase in the allocation of national resources for securing cyberspace.[2] In view of this intensive activity, it is worthwhile to ask how a state can achieve an advantage within the existing cyber arms race.

In this article, I will argue that "Cyber-Dominance" is not only a reflection of the technological development of new and more advanced tools and the operational experience in cyberspace, but also by organization and methods of the security forces and military units in this space, coordinating between the political and military echelons to reflect the changing cyber threat on the countries and the necessary military action. In other words, because we live in a period in which cyber warfare capabilities can be developed relatively easily and the level of sophistication required of the attacker is declining, the distinguishing factor between countries and other international players

[1] The following are several known examples of this: Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington: CCSA Publication, 2013); Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2007); Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2009); Ben Buchanan, *The Cybersecurity Dilemma: Hacking Trust and Fears between Nations* (New York: Oxford University Press, 2016); P. W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What everyone Needs to Know* (Oxford: Oxford University Press, 2014); Harris Shane, *@ War: The Rise of the Military-Internet Complex* (New York: Mariner Books, 2015).

[2] This can be seen in the figures of international insurance companies. See, for example, "Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Future," *Atlantic Council and Zurich Insurance Group Report*, September 10, 2015, Figure 13, http://publications.atlanticcouncil.org/cyberrisks/.

in cyberspace may be the investment in organizational processes and the building of force to achieve a political advantage in cyberspace.[3]

Although the article is not based on a comparative study,[4] the American example, which will be described extensively below, is significant, because it indicates a conceptual and organizational change. In this framework, the United States adopted an approach that regards the cyber realm as cyberspace, or more accurately, as a cyber battlefield.[5] This is the basis for the current military concept in the United States, which led to the organization of American cyber force. This battlefield requires integrated state and military action, similar to the action required to preserve the territorial security and interests of a country in physical space—the air, sea, and land.[6] This assertion will be tested in the article by analyzing the development of the security approach, especially the organization and force building in the cyber realm, as reflected in unclassified official documents. This analysis will be presented according to three timeframes: The first is 1983–1998, when the process of realizing the potential risks posed by the cyber realm to state interests began, and American intelligence units were organized to safeguard sensitive information existing in different computer-mediated communications systems. The second is 1998–2008, when the American defense establishment realized the significance of computer-mediated communications systems and their consequences for the regular functioning of critical infrastructure and key resources needed in a modern country (e.g., water and food, energy, and transportation). The third is 2008–2012, when the concept of cyberspace was

[3] The term "organization and force building" refers to the process of planning, change, and arranging responsibility among various agencies in a specific area of warfare for the purpose of control, command, and development of special personnel, weapons, and doctrine.

[4] For a comparison of cybersecurity policies in the United States, Israel, and China, see Amit Sheniak, "Cyberspace as a Border Area: Creating Sovereignty and Enforcement Capability in Cyberspace in Israel, the United States, and China," published by the author, Jerusalem, 2015 (in Hebrew).

[5] This approach is also reflected in a change in the definition of the professional terms that currently refer to cyber as an environment, dimension, or space.

[6] It should be noted that several studies dealing with the use of language, metaphors, images, and models from other security spheres and technologies, especially nuclear weapons, also mention the importance of the conceptual change in cybersecurity. They do not, however, emphasize the organizational and institutional change on which this article focuses.

revolutionized, and the attitude that was adopted was that military effort in this sphere was an endeavor comparable and tangential to other dimensions (sea, air, and land).

The survey presented in this article indicates that the logic guiding the force building for action in cyberspace among countries and powers like the United States has undergone changes over the past thirty years, given the increase in cyber threats and their effect on a range of state interests. These changes support the article's assertion that the United States is the leading player in the cybersecurity field, to a large extent because it has reorganized its military cyber force based on the same logic that guided the organizing of its aerial, naval, and ground forces. The article does not intend to analyze the disputes within the military and security personal about the advantages and disadvantages of different approaches to organization of force building in the cyber realm or to reconcile them.[7] Rather, the article seeks to highlight the importance of moving ahead with the organization of a national cyber force under the notion that the cyber realm is a battlefield comparable to physical battlefields. This contrasts with the prevailing idea among cybersecurity researchers and decision makers today who focus on technological development and operational experience as the important tools and as the main foci of investment for gaining an advantage in this field.[8]

It can be argued that this organizing concept of cyber power distinguishes between military action of countries leading in cybersecurity (such as the United States) from other political entities and from state, super-state, and sub-state players. The leading countries conduct a regular and coordinated military effort, executing plans and orders that are aimed at achieving a specific tactical and or strategic goal in cyberspace (similar to aerial, naval, and ground operations). Other entities operate irregularly in cyberspace in a "parasitic" network pattern similar to terrorist actions and guerilla warfare, seeking to sabotage, disrupt, intimidate, and influence consciousness by means of computerized communications.

[7] For example, on the question of whether defensive, offensive, and intelligence gathering personnel should be integrated in the agency, whether the dominance of intelligence or technological personnel should be maintained, and so forth.

[8] See, for example, the trend towards technological analysis in articles in cyber policy journals such as *Cybersecurity Journal* and *Journal of Cyber Policy*, which emphasize technological development and operational experience as important tools in assessing and promoting cybersecurity.

1983–1998: The Information Security Concept

The perception of the threat to information and communications technology (ICT) and accordingly the US organization and force building in cyberspace shifted between 1983, when the US military computer system (Milnet) separated from the civilian computer network, and 1998 when the characteristics of the threat had changed. The crux of the change resulted from a more ambivalent attitude towards the advantages and disadvantages of computer-mediated communications technology. This was reflected in a shift from state actions designed in principle to improve and streamline the flow of information to operations aimed at creating control, command, and barriers for protecting sensitive state information (defense and civilian).

The practical significance of the US force building in cyberspace was then reflected mainly by defensive operations for securing sensitive information, such as information collected by armies and intelligence agencies; and computer databases, which over the years became the main means of storing and managing this information. The main actions taken vis-à-vis the computer networks of the intelligence organizations and the army were to upgrade the ability to control secret and classified information (for example, by creating a separate and closed communications network for the army), and for the first time, to obtain valuable covert information within the framework of intelligence and information warfare for formulating the state's legal authority needed for this action. During this period, special institutions and units were founded; the definitions of the responsibility of existing government and defense agencies were changed; and legislation was passed that banned unauthorized entry into sensitive computerized databases and permitted punishment and enforcement. These changes nevertheless did not lead to a substantial shift in military thinking.

The physical and institutional separation between military and civilian computer-mediated communications greatly affected the control and security of computerized information. A series of actions led to this separation, namely the removal of the military communications system from the civilian communications system in 1983; the creation of a classification system that only allowed people in relevant jobs to operate within it;[9] legislation in 1984 that forbade civilians without permission from entering into federal systems

[9] Tamar Ashuri, *From the Telegraph to the Computer: A History of Electronic Media* (Tel Aviv: Riesling Publishing, 2011), p. 138 (in Hebrew).

(defined as "protected computers");[10] and expanding the authority of the American Secret Service to protect these systems.[11]

Reports of espionage and criminal cases of breaking into computer systems, such as the "Cuckoo's Egg"[12] and the arrest of the "414 Gang" in 1983, brought about additional legislation called the Computer Security Act of 1987,[13] which mandated the development of criteria and standards for securing computerized information in the federal authorities;[14] the training of special personnel; and instruction of employees about the potential risks of the computer systems.[15] In addition, the same law stated that the civilian bureaucratic system would be subject to the supervision and instruction of the National Security Agency (NSA).[16] This subordination, which is one of the main institutional changes created then and enforced to this day, was given added validity by Presidential National Security Directive 42 in 1990, which ordered the strengthening of security for national communications systems and the differentiation of those systems from other public communications systems.[17] This directive placed the head of the NSA as the senior supervisory authority for all government departments, by means of a committee led by the secretary of defense established in the framework of the National Security Council.[18]

In 1988, following the public storm caused by the destructive effect of one of the first computer viruses—the Morris worm—which damaged 10 percent of all the computers that were connected to the internet at that time,[19] a Computer Emergency Response Team (CERT) was founded at the initiative of the Software Engineering Institute (SEI) at Carnegie Mellon University to

[10] 18 U.S.C. § 1030: Fraud and related activity in connection with computers, §a2C, (1986).

[11] Ibid., §D.

[12] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage* (New York: Doubleday, 1989).

[13] Computer Security Act of 1987, Public Law No. 100-235 (H.R. 145), (1988).

[14] Ibid, paragraph 1.

[15] Ibid.

[16] Ibid, paragraph 5.

[17] The White House Office, "National Security Directive No. 42: National Policy for the Security of National Security Telecommunications and Information Systems," (1990), §2.

[18] Ibid., §§4–6.

[19] Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 26.

deal with and minimize damage caused by attacks via computers. Although an academic institution took the initiative for establishing the center, the US administration worked to enforce and regulate its activity as the administration usually did with academic institutions—through a contract that stipulated that the US Department of Defense would fund its activity but would also define the framework for its actions.[20] The center later constituted the model for the frameworks of supervising and monitoring threats in cyberspace in the United States and many other countries.

During this period, the prevailing concept regarded the internet as a tool for enhancing capabilities in physical space and not necessarily as a new space for maneuvering between countries. This originated with the security approach and the American military doctrine published in 1996, which had been formulated by the US Armed Forces Joint Chiefs of Staff in their vision about the needs of the future battlefield by 2010. Even though computerized capabilities were already significant at the time,[21] the internet—which was conceptualized for the first time in the military framework as a "network of networks"— was perceived mainly as basic infrastructure that facilitated the ability to use advanced weapons based on an information grid.[22]

This doctrine led to the establishment in 1995 in the US Air Force of a special unit for defensive and offensive warfare using computer-mediated communications, called the 609th Information Warfare Squadron.[23] The highest command regarded fighting by means of computers as only another form of warfare and not as an independent battlefield with its own defensive and offensive efforts,[24] which therefore required the reorganizing of the military

[20] "US Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center," *SEI Press Release*, September 15, 2003, http://www.sei.cmu.edu/newsitems/uscert.cfm.

[21] For example, the defense of computerized infrastructure was addressed in the joint chief of staff's document, but it was mentioned as a tool whose main purpose was to enable superiority in information warfare.

[22] US Office of the Joint Chiefs of Staff, "Joint Vision 2010," (1996), p. 16.

[23] The unit operated from 1995 until 1999, when it was subordinated to the new military organization in cyber warfare. For the official history of the unit, see US Department of the Air Force, "609th IWS: A Brief History, October 1995–June 1999," (1999).

[24] It should be noted that in contrast to this concept, the working echelons that founded the 609th Information Warfare Squadron realized that they were pioneers of the new battlefield. They even compared themselves to the first squadron that developed the theory of air warfare in 1913. See Ibid., p.1.

force.[25] This approach is expressed in an official memorandum published by the Air Force commander and the secretary of the Air Force in 1997, which stated that "information warfare is a means, not an end, in precisely the same manner that air warfare is a mean, not an end."[26] The quote indicates that military thinking did not realize the importance of the concepts of "space" or "dimension" as a basis for determining defense policy in general (not only in the air or only in the cyber realm). It is possible that even today, there are those operating aerial, naval, and ground weapons who regard cyber operations as merely an act of support. At the same time, however, the approach of the writers of the memorandum held that the cyber threat was aimed only at information, and they had difficulty in predicting the extent of the current military endeavor in the cyber realm.

1998–2008: The Infrastructure Concept

During this period, the threat posed by computer networks shifted significantly, both in terms of the level of urgency and the risk posed to a state's sovereignty and its ability to function under attack. The reason for this shift was the changing technical characteristics of hacking into computer systems, which became increasingly complex, while the level of technical sophistication and knowledge needed by parties that committed the hacking declined substantially from the mid-1990s.[27]

A number of hacking events into the Pentagon computer systems in the late 1990s, both in the framework of the ER97 military exercise and in the Solar Sunrise espionage affair, were a wakeup call to the American defense system. These events also made it clear that the US military and security system did not have a single entity responsible for operations against threats of this type.[28] In November 1998, a special task force—the Joint Task Force for Computer Network Defense (JTF-CND)— was created, which

[25] Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 31.

[26] US Department of the Air Force, "Cornerstones of Information Warfare," (1997), http://www.c4i.org/cornerstones.html.

[27] US Department of Homeland Security, "Securing the Nation's Critical Cyber Infrastructure," (2010), p. 3. Note the graph on page 3, which marks the balance between the knowledge needed by the attacker and the level of sophistication of the attack in 1990s. In 1995, ready-to-use sophisticated attack tools could already be purchased.

[28] Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 36.

was subordinated to the Defense Information Systems Agency and later to the US Space Command. The task force acted in synchronization with the NSA and was designated for cyber warfare and for dealing aggressively (not passively) with attacks by foreign countries in order to secure computer networks.[29] This force, which was dismantled in 2010, was an important factor in promoting the readiness of the United States to defend itself in cyberspace, particularly as a result of the diverse and relevant personnel that established bodies capable of coping with offensive computer operations: computer specialists, military personnel from a variety of armed forces branches, intelligence personnel, and security personnel. Later, military personnel were also sent for advanced computer studies, creating an ideal combination with their professional training.[30]

In 2004, the task force assumed responsibility for all defensive and offensive operations in the cyber realm. It shifted from being directly involved in these areas to becoming a regular military staff agency that did not itself engage in defense or attack but rather synchronized and guided all the operative headquarters and tactical units responsible for security operations in cyberspace in the various branches and departments.[31] The new agency—JTF-CNO—led changes in both the bureaucracy-organization and in the practical defensive capability of the American security system. From an organizational standpoint, these changes were the turning point that later led to the establishment of the Cyber Command; from a practical standpoint, the task force—which had originally been formed to deal with security challenges—also achieved significance in capacity building for handling tangential matters that were not part of its original purpose but that jeopardized operational readiness and US sovereignty in cyberspace. Among other things, this involved independent viruses that contributed to the feeling of being under threat, due to the possible consequences of damage to computer-mediated communications.

This new perceived threat led to recognizing the need for an ongoing national status assessment to detect security problems in computer-mediated communications, as a tool for designing policy, and for planning and handling these problems. The assessment revealed that the main weak point was the

[29] Ibid., pp. 38–40.

[30] Ibid., pp. 38–39.

[31] Ibid., p. 57.

country's critical infrastructure and basic civilian resources, which were not protected and not subjected to supervision and concealing of information, and were susceptible to possible damage via the computer communications upon which they relied. One measure for handling this risk was the Critical Infrastructure Information Act of 2002. This law defined the term "critical/essential infrastructure information" as part of a plan for dealing with damage to this sensitive infrastructure,[32] and expanded the definition of the term "protected systems" to also include civilian public systems.[33]

In 2003, President George W. Bush and the secretary of Homeland Security issued the Homeland Security Presidential Directive No. 7 (HSPD7), which validated the need for non-military security activity for defending civilian infrastructure. The agencies founded in this framework under the Department of Homeland Security assumed responsibility for the monitoring, planning, guidance, defense, and determining priorities in cyberspace (without operational forces; these were retained by the army and the intelligence agencies). Authority was also delegated to the various governmental departments to conduct a comprehensive survey that would include an assessment and review of all infrastructure and interests within their field of responsibility in order to locate possibilities of attacks against infrastructure by terrorist organizations using computerized means.[34] The directive also created an analogy between damage to computer systems of specific infrastructure and the use of weapons of mass destruction.[35] This comparison had doctrinal significance, as it led to the conclusion that the United States had to undertake the same kind of preparation and level of investment for cyber threats as they did for threats by conventional weapons and ballistic missiles. This comparison also led cyber warfare theory to

[32] The complete definition stated in the law is "Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems." See Homeland Security Act of 2002 – Critical Infrastructure Information Act, Public Law 107-296: Sec. 211/3 (2002).

[33] Ibid., Sec. 211/6.

[34] US Department of Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection," (2003), §12.

[35] Ibid., §13.

widely adopt the Cold War terminology—such as "deterrence" and "active defense"—which is still prevalent to this day.[36]

In 2003, the Bush administration published a national strategy for cybersecurity that was based on a survey of dangers and that included components indicating an important shift in consciousness and organization in both the federal administration and the private sector;[37] the formation of a security response team for cyberattacks on the basis of CERT; a plan for reducing security risks and national weak points vis-à-vis cyber threats; improvement of government cybersecurity; international cooperation for the purpose of improving national cybersecurity; and the establishment of two institutions in order to improve supervision of security for computerized financial infrastructure.[38]

The national strategy for cybersecurity included the private sector as an essential partner in creating security and preserving sovereignty, based on the realization that the steep increase in e-commerce had led to the ability to damage US economic interests. The Presidential Directive EO 13286 in 2003 further legitimized this approach and led to an additional organizational change: the appointment of official agencies to mediate between the defense sector and the private sector, such as the National Infrastructure Advisory Council and the Information Sharing and Analysis Center.[39] Despite the importance of the private sector, the focus of this article on the change in organizing the military force and security agencies does not allow for extensive discussion of the organizational change that was created in order to expand the cooperation between the security and private sectors in the United States, which currently is a key factor in monitoring cyber threats.

Another law from 2004 was designed to reform the American intelligence services so that they could adapt to the current threats.[40] For the first time, the law openly referred to the possibility that the United States would make

[36] For a discussion of the question of deterrence in the cyber realm, see, for example, Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016–2017): 44–71.

[37] The White House, "The National Strategy to Secure Cyberspace," (2003), p. X.

[38] "Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 56.

[39] The White House, "Executive Order No. 13286: Critical Infrastructure Protection in the Information Age," (2003).

[40] Intelligence Reform and Terrorism Prevention Act of 2004, Public Law No. 108-458 (2004).

passive and active use of computer-mediated communications in order to improve its self-defense. The law also mentioned two different types of actions in cyberspace: offensive action against computerized transactions carried out by electronic means and designed to finance trans-border crime and terrorism, and intelligence action for gathering existing information in cyberspace in order to prevent members of terrorist and criminal organizations from entering the United States.[41]

The National Infrastructure Protection Plan[42] was published in 2006. It implemented the above-noted processes of organization and established the Department of Homeland Security as the agency that would coordinate and determine policy for the defense of critical national infrastructure and resources, including coordination between the civilian state bodies and the military and intelligence bodies. The plan defined cyberspace for the first time as critical national infrastructure that should be defended, rather than merely a tool through which infrastructure is damaged.[43]

The transition from policy decisions to reorganization of the military force took place in 2006, following the publication of the "National Military Strategy for Cyberspace Operation," which defined the military knowledge needed for integrating the American army into the efforts to defend cyberspace. This document defined the strategic context, the sensitivities, and the outlines for formulating a plan of action and a special doctrine for regular military activity in cyberspace,[44] but it did not stipulate the formation of a specific general command body for this matter.

2008–2012: The Spatial Concept

This period constitutes the peak of the institutional change in organizing the American forces in the cyber dimension. This change is characterized by two principles derived from the approach that regards cyberspace as militarily important: 1) organizing military power based on a spatial concept

[41] Ibid., Sec. 6302§bl.

[42] The document requires a periodic status assessment, the updated version of which is published every few years. This article relies on a later version of the document from 2009; see US Department of Homeland Security, "National Infrastructure Protection Plan," (2009).

[43] Ibid., §3.2.5.

[44] US Office of the Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations," (2006), p. 1.

(cyberspace); and 2) the cyber dimension as a source of information and social and political interaction, which requires monitoring and supervision in order to maintain state security and promote national interests.

The attitude of the American administration towards the internet as a space having both specific characteristics and a complexity requiring a unique bureaucratic approach is evident in the documents accompanying the 2008 US presidential elections between Obama and McCain. Policy on cyberspace, especially its security dimension, became one of the key issues of that period. As a result, the Center for Strategic and International Studies published a report by cybersecurity experts, which was aimed at the incoming president.[45] The report called for increasing the federal government's involvement in cyberspace and opposed the approach that relied on internal arrangement led by the private sector. The report's recommendations also included a call for creating a balance of deterrence against enemies in cyberspace.

In 2009, at the beginning of Obama's term, the administration published a new policy entitled the "Comprehensive National Cyber Initiative" (CNCI).[46] The declared goals of the CNCI were to set in motion a widespread inter-agency measure aimed at improving the feeling of security in cyberspace among American citizens.[47] In this framework, the plan declared an organizational change in the handling of cyber threats, divided into two main efforts: 1) improving centralization in a way that would raise the level of state control and supervision in the cyber dimension; and 2) strategic planning and management of partnerships with international parties in this area. Improved centralization was reflected by technical development of command and control systems of federal information and computer networks.[48] The strategic planning was manifested by the establishment of institutions for long-term development and procurement that would prevent, among other

[45] Center for Strategic and International Studies, "CSIS Commission on Cybersecurity for the 44th Presidency: Securing Cyberspace," (2008).

[46] The plan was an implementation of President Bush's National Security Presidential Directive (NSPD), no. 54, which President Obama adopted. It included the recommendations of the CSIS report. See the White House, "Comprehensive National Cybersecurity Initiative," (2009), http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[47] Because the plan was an implementation of NSPD no. 54, which was classified in principle and reportedly focused on offensive and intelligence measures, it can be assumed that it also had undisclosed objectives.

[48] "Comprehensive National Cybersecurity Initiative," pp. 2–3.

things, penetration of infected hardware components, and by setting targets for educating the administration's employees to be aware of the need to defend against cyber threats.[49] International partnerships were formed with various parties (countries, companies, and organizations) in order to create deterrent capability in the cyber realm.[50]

The need for regular and orderly strategic planning from the presidency on down was expressed in a series of documents written early during the Obama administration, including a founding document published under the title "Cyberspace Policy Review." This document recommended the establishment of the "Cybersecurity Office" as part of the presidential advisory team, in combination with the National Security Council.[51] The recommendation was applied in the Information and Communications Enhancement Act of 2009,[52] which also stipulated that the presidential cybersecurity advisor would head the Cybersecurity Office and would be part of the president's limited team of advisors.[53] The importance of establishing the Cybersecurity Office lay in improving the coordination and ability to carry out an overall security policy from the level of the president (the commander in chief of the US Armed Forces) to the various security agencies to the army units, and especially the capability to formulate measures for supervision that would be based on the development of standards for security in cyberspace in general and the national information systems in particular.[54]

Another significant result of the measure to centralize the cyber realm was improving the ability to formulate policy for the new legitimate use of force in cyberspace. This resulted from a policy of orderly response led by

[49] Ibid., pp. 4–7.

[50] Ibid., p. 5

[51] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," (2009), p. 7.

[52] The background for the law was a Senate hearing held in 2008 about the capabilities for defending the federal IT infrastructure as well as criticism of the FISMA law from 2002, based on the claim that the measures provided by the law for an assessment were murky and that it was not clear to each agency the extent of the information that it was supposed to oversee. See Information and Communications Enhancement Act of 2009 (S.921/ ICE Act), 111th Congress, Sec. 2/4, 5 (2009).

[53] Ibid., Sect. 3552.

[54] Ibid., Sect. 3556.

the president and was based on a report by the National Research Council,[55] which analyzed the legal and ethical consequences of cyberattacks and recommended that such attacks be perceived as constituting the "use of force," i.e., as justifying a military response (in the physical dimension).[56]

The most significant expression of the organizational and conceptual change relating to the internet as a space has been in the organization of the military forces and the doctrine for their deployment. The most prominent organizational change in the US military, reflecting its recognition of the existence of cyberspace, has been the official establishment of the US Cyber Command (USCYBERCOM). The decision to establish the command was made in 2009, declared operational a year later, and subordinated to the US Strategic Command (USSTRATCOM).[57] The new command was defined as a sub-unified/subordinated command; that is, a military body established by presidential order as a command entrusted with a specific spatial task requiring local expertise and operating under the spatial command of the US Armed Forces.[58]

Although fighting units using computers and computerized communications networks had already existed in the United States since the 1990s (see above about Unit 609), the creation of a sub-unified/subordinated command for this purpose reflected a shift in the concept and had profound symbolic and organizational significance. From an organizational perspective, even though a full spatial command or a branch/corps for cyber operations has still not been established,[59] the new military command currently guides and

[55] This comprehensive report, which was written by a special committee formed by the National Research Council, analyzes many other aspects relating to online attacks in criminal and civil law.

[56] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities* (Washington DC: National Academies Press, 2009), pp. 33–34.

[57] US Department of Defense, "US Cyber Command Fact Sheet," (2010).

[58] Other sub-unified/subordinated commands in the US Armed Forces were established to manage security in Alaska, provide aid in South Korea, and for the war in Afghanistan. See US Office of the Joint Chiefs of Staff, "Joint Publication 1," (2009), p. V–9.

[59] The commands in the US Armed Forces are divided into spatial commands responsible for the use of force in various regions of the world (for example, CENTCOM, the central command, is responsible for the Middle East), and specialist functional commands are responsible for force building, training, and the allocation of forces, such as the Special Forces Command (SOCOM). This second category of commands also includes the conventional branches, such as the Air Force, Navy, and Army.

synchronizes all US military operations in cyberspace and constitutes the headquarters for cyber warfare in the various branches of the Armed Forces (Army, Navy, Air Force, Marines) that are professionally subordinate to it. Furthermore, the US Cyber Command is responsible for finding and developing personnel and weapons and for formulating a doctrine for the cyber realm. The creation of the US Cyber Command is a clear and overt symbol, emphasizing to other countries the advanced stage that the United States has reached in the militarization of cyberspace. This status of the United States as a leading—and possibly the only—military power in cyber warfare has led to similar organizational changes within the armies of other countries (for example, China established its cyber command in 2010).[60]

The organizational change, which culminated in the establishment of the US Cyber Command, accompanied—and possibly also led—a change in the military doctrine as published in official documents of the US joint chiefs of staff. Recognition of cyberspace as a space in which warfare takes place simultaneously with and in addition to the existing battlefields began in 2006, but it appears that this knowledge did not crystallize into a regular doctrine until 2012 when its main points were published.[61] The purpose of this doctrine was to provide integrated guidance to the US Armed Forces on how to carry out offensive and defensive battle operations in cyberspace.[62] The high level of maturity in developing weapons, training personnel, and formulating a special theory of warfare for cyberspace that the American defense establishment had reached since the creation of Cybercom was exposed in 2012 by President Obama in Presidential Policy Directive 20, which deals with offensive activity in the cyber realm, including "active defense."[63] This document, which is classified as "secret," was published in the British newspaper the *Guardian* as part of the documents exposed and leaked by

[60] Tania Branigan, "Chinese Army to Target Cyber War Threat," *Guardian*, July 22, 2010.

[61] US Office of the Joint Chiefs of Staff, "Joint Publication 3-13 Information Operation," (2012).

[62] US Office of the Joint Chiefs of Staff, "Compendium of Key Joint Doctrine Publications," (2014).

[63] The White House, "Presidential Policy Directive 20: US Cyber Operations Policy," (2012).

Edward Snowden.[64] It constitutes substantial evidence of the institutional change that the American defense establishment underwent in its attitude towards computer-mediated communications prior to regarding it as a theater of activity. The presidential directive includes detailed definitions of types of attacks and defensive measures in the cyber realm, including passive network defense, offensive cyber activity, cyber campaigns, intelligence gathering from within or using cyberspace, cyber warfare for defense purposes, non-invasive defensive operations, and so forth.[65] The directive refers to the fact that the United States already had proven offensive capabilities, which it uses to exercise its right to self-defense, following a scrupulous process of authorization.[66]

Another conceptual and organizational change that began during this period, in addition to the concept of cyberspace as comparable to a physical space, was the treatment of cyberspace as an important social and public theater that has both negative and positive potential and requires monitoring and protection. The classification of cyberspace as an infrastructure in its own right—not merely as a space that mediates between interests in physical space—was added in 2010 as part of a policy of the Department of Homeland Security, entitled, "Securing the Nation's Critical Cyber Infrastructure." This plan referred to cyberspace as a social, political, and economic theater, which included countries, criminal elements, terrorist organizations, and individuals.[67]

The defense involvement in social interaction in cyberspace also influenced the revision of the US Armed Forces' doctrine of implementation of information operations. A doctrinal document from 2012 stated that cyberspace was essential for the existence of information operations as part of an ongoing military effort,[68] and that it was one of the channels for influencing the "information environment," because it could be used to both disrupt or prevent

[64] Edward Snowden was a former employee of the CIA and NSA who specialized in online intelligence. In 2012, Snowden leaked a large number of documents to leading global media. The documents exposed the depth of intelligence gathering and active operations by the United States and its allies (the joint intelligence community of the United Kingdom Canada, New Zealand, and Australia) in cyberspace.

[65] "Presidential Policy Directive 20: US Cyber Operations Policy," pp. 2–4.

[66] Ibid., pp. 4–11.

[67] US Department of Homeland Security, "Securing the Nation's Critical Cyber Infrastructure," (2010), pp. 7–10.

[68] US Office of the Joint Chiefs of Staff, "Joint Publication 3–13: Information Operations," (2012), p. III.

messages and to disseminate messages and carry out deception through use of the social media.[69] The treatment of cyberspace in official presentations by the spatial commands of the US Armed Forces, where it was portrayed as a basic part of the operational concept, made it clear that cyberspace had become one of the areas of action of the US military.[70]

In addition, from an organizational standpoint, the United States recognizes that the ability to operate in public-civilian cyberspace is not an exclusive one; therefore, it must cooperate with sub-state and supra-state players, particularly local and international consultancy and software companies that constitute a partner and source of information for improving security in cyberspace, as evident from the recommendations of various official committees and reports.[71] For example, these recommendations indicate that despite the organizational changes that have led to the training of specialist military and government cyber personnel, areas in which external non-military parties have an advantage still exist and that the United States is unable to close this gap in the near future and must therefore rely on the relative advantage of these external parties. This is especially true of areas such as forensic identification, for which there is still no solution at the state level.[72]

Force Building in the Cyber Domain as an Expression of Organizational Conceptual Change

In February 2016, President Obama published an "Op-Ed" in the *Wall Street Journal*, in which he argued that the United States should allocate more money to the development of technologies for cyber defense, with an emphasis on protecting government information systems infrastructure.[73] The publication of the article slightly predated the US administration's

[69] Ibid., p. II–9.

[70] See, for example, "The Operational Art of Fighting in and Through Cyberspace (Unclassified PP presentation)," slide 12, a non-classified conceptual presentation prepared for General Moulton, head of planning and operations in the European Command of the US Armed Forces, given to a college of Army officers.

[71] Center for Strategic and International Studies, "CSIS Commission on Cybersecurity for the 44th Presidency: Human Capital Crisis in Cybersecurity," (2010), p. VIII.

[72] For example, virus activity was exposed by commercial companies specializing in the field, such as Kaspersky Lab and others.

[73] Barak Obama, "Protecting US Innovation from Cyberthreat," *Wall Street Journal*, February 9, 2016, http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

decision to increase spending by $19 billion on the development of these technologies.[74] President Obama's article represents the prevailing approach especially among decision makers in the United States and most likely in other countries; it relies on the assumption that the panacea for the growing difficulty of securing cyberspace and protecting critical national infrastructure and resources is to increase technological development and invest resources in it. Although Obama states in his article that senior defense establishment officials and military officers would apply the spatial organizational approach, it appears that this currently has not prevailed among US decision makers.

As noted above, studies in defense and international relations in recent years have dealt at length with the development of warfare in cyberspace, and the desirable state strategy.[75] It should therefore be asked: What is the significance of focusing on organizational and conceptual change instead of technological development? Specifically, what is the optimal way of organization in order to achieve a security advantage in cyberspace? What contribution does describing this process have on understanding and improving a country's capability in providing security for its citizens against cyber threats?

In the following discussion, the article presents an alternative to the latter, stressing the benefits of investing in organizational development and highlights the possible different consequences of the two choices. Although it is not based on a comparative research, this discussion has value for understanding the different level of dominance in the cyber domain achieved by other countries that decided to prioritize organizational and conceptual development over technological development. At the onset of the article, it was noted that the current focus should be on re-organizing the forces to provide security in cyberspace as did the American military., which regards cyberspace as a battlefield comparable to physical battlefields. I believe that the need for this focus lies in two complementary factors: 1) the growing threats posed by cyberspace and the changes that have occurred to those

[74] Tobias Naegele, "7 Keys to President Obama's 19 Billion Cybersecurity Plan," *GOVTECH Works*, February 16, 2016, https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.iMSThHM.

[75] See, for example, the discussion of the ability to defend against cyberattacks utilizing the Internet of Things (IoT) in Bruce Schneier, "Security and the Internet of Things," *Schneier on Security, February 1, 2017,* https://www.schneier.com/blog/archives/2017/02/security_and_th.html, and the discussion of deterrent capability in cyberspace in Nye, "Deterrence and Dissuasion in Cyberspace," pp. 44–71.

threats; and 2) the unique technological characteristics of the weapons in cyberspace.

In regard to the first factor of the change in the threat, the examples from the three periods described above highlight the organizational shifts that have occurred in the US defense establishment due to the growing comprehension of the depth and substance of the threat in cyberspace to the security policies in general and to the ability to use military force in particular. The source of the change lies in the transition of cyberspace as a system for transmitting information to an important omnipresent element in modern life. Cyber began as a threat posed by other countries or individuals to sensitive and covert state information—such as official state information, intelligence, and technological knowledge, all defined as part of the "information security"—to threatening the basic infrastructure and fundamental resources of a modern country that relies on computerized information, and can be defined as part of the defense of strategic infrastructure and sites (civil defense); finally, it has become a spatial threat (cyberspace), which interacts with and affects a large proportion of civilian and military operations in physical spaces. The latter can be described as a threat to a country's sovereignty and to interpersonal interactions—economic, political, and social—that is, a threat to the public security. The diverse human use of cyberspace means that it is no longer possible to focus on defense of state infrastructure solely by means of technological development (as indicated by President Obama's statement).

The second factor that contributed to the uniqueness of weapons in cyberspace, results from their rapid technological development and their growing availability in the private market, as evident from the daily need to update hardware and software at a quick pace in the home computer system. The development of computerized espionage and surveillance tools, easily obtainable in the private sector and simple to use,[76] has prevented countries from achieving a technological advantage through the national development of new weapons. A state cannot cope with the rate of development and the relatively low prices of similar weapons in the private market; therefore, development alone cannot be the only or even the principal means of achieving an advantage in the cyber domain. This unique characteristic leads to the conclusion that the ability to control and defend cyberspace cannot be based

[76] The US administration has already recognized this problem. See, for example, "Securing the Nation's Critical Cyber Infrastructure," (2008). p. 3, Figure 1.

solely on technological development but must also include organization of force and the evolution of a doctrine that employs force in a way in which it will be well integrated with a country's other military actions. This approach is similar to the organization of force for creating security in physical space, such as organizing an air force to protect the national air space and to assist ground and maritime efforts. Comparing between the virtual space and the physical space—between a field perceived as new and revolutionary and the "old and conservative" mode of action—is part of the necessary solution.

The historical review presented above shows that the spatial organizational approach is the one being applied by the American security bureaucracy, especially the military. Its clearest practical expression is the formation of a designated, extensive, and solid security establishment in cyberspace, which includes a number of special personnel operating hierarchically from the level of a consultant office in the president's staff to military units and the United States Computer Emergency Readiness Team (US-CERT). Operations are also coordinated with policing units and divisions in the Department of Homeland Security, and with semi-governmental bodies that mediate between the public and private sectors.[77] This characteristic has also led to a change in the use of force in cyberspace: from targeting sensitive information and national infrastructures to effecting the adversary's internal legitimacy.

It is possible that the spatial organizational change is also one of the reasons for the hierarchy in the power relations between the various countries operating in cyberspace. This change is one of the special characteristics of great international powers (GPs) like the United States, which is the leading international security force in cyberspace, capable of allocating resources for organizing military action based on a spatial-like principle. This kind of change is expensive, requiring personnel, expertise, and organizational capabilities that are unique to states that are accustomed to large-scale security spending. In other words, asymmetric operations in cyberspace, such as terrorism, sabotage, theft of information, psychological warfare, and fake news-type communications can be executed by weak states and even non-state organizations. The ability to organize operations in cyberspace as regular military missions based on the spatial organizational approach is

[77] (NCSC) National Computer Security Center; (NIAC) National Infrastructure Advisory Council including the business sector and higher education; (ISAC) Information Sharing and Analysis Center.

confined to global and regional powers and a few other countries possessing technologically advanced modern armies.

The question of whether we are witnessing an organizational competition between the Western style of organization of force in the cyber domain by forming official state military and security institutions—in which the United States is the leader—and the hybrid organizational concept of carrying out offensive cyber action using an "Ecosystem" that synchronizes state security institutions, universities, the private sector and/or criminal elements—led by countries like China and Russia—requires additional research that could be an important future contribution.

Given the changes in the organization of the cyber capabilities as part of military force, one could ask the question arises of whether it can be assessed using the same tools through which we measure force building in the physical space and whether we can compare the two. The answer is not unequivocal. On the one hand, from the perspective of cost-benefit calculations, it is clearly impossible to compare the cost of a new aerial platform, either monetarily or in terms of development resources and professional investment, and the development of operational cyber tools. On the other hand, in both cases, force building involves the need to develop the capacity of using the weapons in combination with existing weapons that are designed for warfare in a different space by means of procedures, doctrine, and technological tools that enable better command and control. Historical comparisons can also be made between the development of aerial and naval military combat systems, and the development of cyber combat systems as a result of technological advancements.[78] Such a comparison emphasizes the importance of both the organization of force around a spatial concept in the cyber domain as a way of achieving a national security.

Summary and Conclusion

The organizational change in the United States due to the emergence of the concept of "cyberspace" has led to transformations in three areas: in the

[78] This question has begun to attract the attention of researchers in recent years. See, for example, Amit Shiniak, "The State Plan in the Online Border Zone: A Theoretical and Historical Comparison," *Bein Ha-qtavim*, (Dado Center for Interdisciplinary Military Studies), no. 3 (2014): 13–44 (in Hebrew); Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," Cyber Studies Programme, Working Paper Series No. 1, University of Oxford, March 2015.

range of cyber operations; in the characteristics of these operations; and in the conception of activity in cyberspace and its consequences for the United States' national security approach and its overall strategy. The development of the range of US security operations in cyberspace, which initially were limited, restricted, and aimed mainly at securing and protecting the national cyberspace (institutions and interests) and have culminated with US forces prepared to conduct offensive, defensive, and intelligence cyber operation, resulted mainly from an organizational change. This has led to the creation of units, agencies, and organizations with defined responsibilities and a national mechanism for coordinating the activity in cyberspace.

Despite this development, organizational change has not been sufficiently recognized in research nor professional frameworks, and important budget decisions, such as the one by the Obama administration, reflect the belief that investment in technological development alone will lead to a better security of the cyberspace. This approach contradicts the substantial development in the force organization in cyberspace, as described in this article, and jeopardizes its continuation. It is also the result of a bureaucratic attitude that tends to assess policy through quantitative (cost-benefit) measures, while ignoring qualitative aspects, such as conceptualization, organization, and doctrine creation, which are some of the qualitative elements that give an advantage to companies using weapons in every space, including cyberspace.

The final conclusion of this article is that in the framework of planning today's security strategy, it is worthwhile also to address the differences between states in their ability to organize defense operations in cyberspace, with an emphasis on regional powers and the world's leading military forces. The process of organizing and consolidating the spatial operating concept that characterizes current US military policy is part of the creation and consolidation of behavioral norms. These organizational norms are the subject of the current international discourse on cyberspace and are worthy of study and research and of becoming part of the assessment mechanism in the development of capabilities in this sphere. This article recommends an organizational approach based, to some extent, on equivalence between states conduct in cyberspace and in physical spaces, in order to make it possible to develop multi-dimensional control capabilities for managing an "integrated," synchronized physical and technological operations that might lead eventually to a national dominance in cyberspace.

The Vulnerable Architecture of Unmanned Aerial Systems: Mapping and Mitigating Cyberattack Threats

Gabriel Boulianne Gobeil and Liran Antebi

Unmanned aerial vehicles (UAVs), frequently referred to as drones, have become an essential and dominant tool of advanced military forces, especially those engaged in counterinsurgency, where they are used mostly for intelligence, surveillance, and reconnaissance (ISR) missions as well as for different kinds of operations involving targeted strikes. As the usage of unmanned systems for military purposes increases, so does their vulnerability to cyberattacks, the result of their growing dependence on computer-based systems. The article maps the different kinds of plausible cyberattacks targeting UAV systems, assesses their odds, and offers some guidelines for a recommended policy for the users of those systems.

Keywords: Cyberattacks, cybersecurity, military technology, unmanned aerial vehicles (UAVs)

Gabriel Boulianne Gobeil is a B.C.L./LL.B. Candidate at the Faculty of Law, McGill University. He has an MA in Security and Diplomacy from Tel Aviv University and an MA in Political Science from the University of Ottawa. Dr. Liran Antebi is a research fellow at the INSS, a lecturer in the academia and a member of IPRAW (The International Panel on the Regulation of Autonomous Weapons).The authors would like to thank Mr. Niv David for helpful comments on an earlier draft of this article.

Introduction

The role played by unmanned aerial vehicles (UAVs) in contemporary warfare has grown since they were first widely deployed in the early 1970s.[1] Primarily used by the US military, Daniel L. Byman even refers to them as Washington's "weapon of choice."[2] Their unmanned nature, enabling the projection of force without the need to send soldiers in physical harm's way, has rendered them quite appealing to other actors.[3] However, the feature that enables them to be operated from a distance potentially represents a double-edged sword, as it leaves the technology particularly vulnerable to cyber threats. Although the fact that UAVs are highly computerized and gives them the advantage of not requiring human operators in the cockpit, this characteristic also allows hackers to exploit UAV systems. This paper calls attention to these vulnerabilities; by being aware of the system's vulnerabilities, the UAV user is more likely to be prepared to prevent and protect against potential cyberattacks.

This paper begins by examining the various components involved in the broader operation of a UAV. By deconstructing the system, we can understand the UAV's vulnerability to potential cyber intrusion. Although hackers seek to gain access to the system itself, they do so by using at least one component as a point of entry into the larger system. The paper then highlights cyberattacks targeting UAV systems, which have either been recorded in the past or are technologically plausible. While some cyberattacks may be performed by individual hackers, more sophisticated attacks require advanced abilities and can only be performed by actors possessing greater resources, such as terrorist organizations, companies, or even states. Yet, as the article will show, even the least sophisticated cyberattacks can pose a serious risk to the user of UAVs. The paper concludes by offering policy recommendations to mitigate the threats stemming from these cyberattacks.

[1] Ty McCormick, "Lethal Autonomy," *Foreign Policy* 204 (2013): 18–19.

[2] Daniel L. Byman, "Why Drones Work: The Case for Washington's Weapon of Choice," Brookings Institution, June 17, 2013, accessed June 5, 2017, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice/.

[3] See Sarah Kreps, *Drones: What Everyone Needs to Know* (Oxford: Oxford University Press, 2016), p. 60.

Research Questions and Structure of the Paper

The current literature on unmanned aerial vehicles (UAVs), which has burgeoned over the last five years, has investigated several important questions, especially related to the use of UAVs in targeted killing campaigns.[4] In particular, a significant portion of this literature has attempted to determine whether UAV strikes used to decimate terrorist organizations are strategically effective.[5] Additional work has examined whether the ways in which UAVs have been employed thus far comply with international legal and ethical standards, in an attempt to understand the various implications of the technology's different uses.[6]

Scholars, however, have not offered any extensive account of the limitations that are inherent to the technical architecture of UAVs, except for cursorily acknowledging that UAVs are susceptible to cyberattacks.[7] Thus, the main objective of this paper is to fill this void and, in doing so, contribute to bringing the academic literature on UAVs into conversation with current work in an emerging area of research in security studies, namely cybersecurity.

[4] Often referred to as drones, UAVs are not actually unmanned, as a human operator controls them from a distance. Hence, a more accurate designation would be "remotely controlled aircrafts." However, given that this is not commonly used in the literature, this paper uses the more widely recognized term UAV.

[5] Stephanie Carvin, "The Trouble with Targeted Killing," *Security Studies* 21 (2012); Matt Frankel, "The ABCs of HVT: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists," *Studies in Conflict and Terrorism* 34 (2011); Jenna Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes," *International Security* 38, no. 4 (2014); Avery Plaw, "Terminating Terror: The Legality, Ethics and Effectiveness of Targeting Terrorists," *Theoria: A Journal of Social and Political Theory* 114 (2007); Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism," *International Security* 36, no. 4 (2012).

[6] Grégoire Chamayou, *Théorie du drone* (Paris : La Fabrique éditions, 2013); John Krag and Sarah Krebs, *Drone Warfare* (Cambridge: Polity, 2014).

[7] Kagu and Kreps, *Drone Warfare*, pp. 44–45; Kreps, *Drones*, p. 39; Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009), p. 253; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), pp. 314–315; Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), p. 23, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

As such, this paper is divided in three parts. The **first** section explains how UAVs and the larger system to which they are integral work. This discussion represents a necessary step to addressing the paper's main research question, which is posed in the **second** section**:** What are the vulnerabilities that stem from the way UAVs work? Having identified these vulnerabilities, the **third** part of the paper tackles another important question: How can the threats posed by these vulnerabilities be mitigated? In identifying the cyber vulnerabilities of UAVs, the broader objective of this paper is to understand how the architecture of the UAV's technology makes it susceptible to exploitation by diverse cyberattacks so that accessible policy recommendations can be offered to help reduce the cyber risks involved in using UAVs.

The scope of this paper is limited to UAVs classified by the US army as "Group 4" and "Group 5."[8] These two groups include UAVs that weigh above 1320 pounds and can fly at altitudes of *up to* 18000 feet for those in Group 4 and *above* 18000 feet for those in Group 5. UAVs such as the Predator, the Reaper, and the Global Hawk are all currently used by the US army and fall under these two categories, and therefore are the focus of this paper. Smaller UAVs, which require a direct line of sight and whose architecture is therefore distinct from those of Group 4 and 5, will not be discussed in this paper. This omission is not because UAVs of Groups 1 to 3 cannot be hacked. As opposed to UAVs of Groups 4 and 5 that are used strategically, UAVs from Groups 1 to 3 tend to fulfill tactical purposes, as is the case of the Raven, for instance. Thus, devoting resources to defend them against a wide range of cyberattacks likely would be ineffective in terms of cost because doing so could diminish the effectiveness of the UAVs, which stems from their being light, portable, relatively inexpensive, and not too sophisticated. In other words, by choosing to use a Raven, the user willingly opts for an UAV designed to provide certain tactical advantages that would be undermined by the addition of a complex defense mechanism.

Moreover, this paper focuses exclusively on UAVs from Groups 4 and 5 because, unlike their counterparts from Groups 1 to 3, they are highly computerized and made of even more sub-systems, rendering them particularly vulnerable to cyberattacks. UAVs classified as Groups 4 and 5 also bear higher risk given that they can be equipped with missiles and deployed for

[8] United States Army, "“Eyes of the Army”: U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035," (2010): 12.

targeted killing missions, unlike UAVs classified as Groups 1 to 3. Moreover, more advanced weapons platforms warrant special attention since their vulnerabilities can result in greater financial and security risk, when compared to the risk imposition of less advanced systems such as UAVs from Groups 1 to 3. The addition of defense mechanism to UAVs from Groups 4 to 5 will inevitably come at the price of reducing their effectiveness, such as when the encryption of a satellite datalink to secure the transmission of sensitive information concomitantly forces the user to spend more time decrypting that information; yet, these costs are outweighed by the advantages they bring to the overall security of the system.

In the technological interactivity of war, the advent of UAVs has offered important advantages. One obvious benefit is removing soldiers from the physical battlefield. Additionally, their technological complexity relies on computer networks—often referred to as "unmanned aerial systems"[9]—rendering their reproduction technically burdensome.[10] As relatively sophisticated technologies, UAVs necessitate substantial resources and knowledge to build and operate. Furthermore, their airborne platform, flying at relatively high altitudes, makes them more difficult to attack via kinetic means, and thus demand more advanced capabilities to take them down. For these reasons, actors seeking to attack them are likely to look for alternatives in the cyber world. Cyberattacks present a likely substitute for kinetic attacks because the architecture of UAVs—that is, their reliance on computer networks—makes them inherently vulnerable to hackers seeking to exploit the technology's limitations. Therefore, it becomes important for the user of UAVs to understand how the technology can be exploited so that the threats that arise can ultimately be mitigated. These interactions between users and hackers of UAVs deserve special attention—both within national security and academic circles—a task to which this paper is devoted.

Three Central Components of the UAV System: How UAVs Work?

UAVs are part of a complex system that consists of several interconnected and integrated elements, all of which are needed for the UAV to conduct an intelligence, surveillance, and reconnaissance (ISR) mission, or to locate

[9] Kagu and Kreps, *Drone Warfare*, pp. 49–50.

[10] Kreps, *Drones*, p. 63.

and hit its target. Although this system contains several parts, this paper focuses exclusively on the following three components: (1) a military base or a command and control center from where the operator controls the UAV; (2) a satellite that connects the UAV to the command and control center; and (3) the UAV or aircraft itself.[11] These components are based on the US Air Force Road Map, which regards Predators and Reapers as more than individual aircrafts, and as complete "systems" in and of themselves.[12]

Another ground base, called a launch-and-recovery station, is also essential for the UAV to take off and land before and after missions. Such stations, which may also be an aircraft carrier from where the UAV is refueled and stored when not in operation, are also a part of the system. They are not discussed here, however, because they are less likely to be targeted by *cyber*attacks as opposed to *kinetic* attacks.

Moreover, each part of the UAV system contains smaller technologies that may be subject to cyberattacks. For instance, the command and control center is equipped with several communication technologies that enable communication with the UAV, each of which can be individually targeted by hackers. As is briefly addressed below, missiles or payloads carried by UAVs can also be the object of cyberattacks. That said, the countless ways in which the myriad parts within the whole system can be hacked is beyond this paper's scope. Conceiving of UAV systems as being made of the abovementioned three components is therefore sufficient to enable the reader to identify the main points of entry into the UAV in the event of a cyberattack.

[11] See United States Air Force, "MQ-9 Reaper." Refer to Image 1 for a visual representation of the three parts of the system. For other useful graphical representations of this system, see *Eye in the Sky*, directed by Gavin Hood (Toronto: Entertainment One, 2015); Derek Gregory, "From a View to a Kill: Drones and Late Modern War," *Theory, Culture and Society* 28, no. 7–8 (2011): 197; Ian G. R. Shaw, "The Rise of the Predator Empire: Tracing the History of U.S. Drones," *Understanding Empire*, 2014, accessed December 30, 2016, https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/.

[12] United States Air Force, "MQ-1B Predator," 2015, accessed December 31, 2016, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx; United States Air Force, "MQ-9 Reaper," 2015, accessed December 31, 2016, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx.

Component 1: The command and control center

The first component of the system—**the command and control center**—is where pilots and operators control and supervise the system from a distance, on the ground. Although a command and control center located in the United States, for example, might reduce the exposure of the crew to physical harm, it is likely to be the target of cyberattacks. Command and control centers are equipped with numerous computers and other technologies, and they are essential for the operation of the UAVs but also vulnerable to external and internal cyber intrusion.

Component 2: The satellite

Unlike smaller UAVs, which depend on a radio signal to be maneuvered and typically remain in the operator's direct line of sight, the UAVs classified by the US army as Groups 4 and 5 depend on **satellites**—the second component of the system—that act as an intermediary between the UAVs themselves and their operators. These satellites facilitate the transmission of images and data captured by the cameras and sensors installed on the UAVs, from the aircraft to the command and control center; and likewise, vice-versa, transmitting commands from the base back to the UAVs. The satellite is a crucial part of the system because it provides the UAV and its operator with the precise geographical position of the aircraft, facilitating the UAV to locate its target. Moreover, as Ian G. R. Shaw notes, the use of satellites to connect UAVs to their operators is precisely what allows for the significant increase in the distance between these two parts of the broader system.[13] In fact, he explains that prior to the use of satellites, UAVs had a short command and control datalink that would have made it impossible to operate a UAV in the Middle East from a base located in the United States, as is now the case with Predators, Reapers, and Global Hawk.

In short, the satellite performs two key functions for the UAV: it is the integral part of its GPS navigation, and it acts as the main communication channel for all data exchange between the aircraft and the human operators. Because it relays such crucial information, the datalink that passes through the satellite represents a strategic target for any hacker seeking to disturb or disrupt any UAV operations (These real eventualities are discussed in more details in the next section of the paper).

[13] Shaw, "The Rise."

Component 3: The aircraft (UAV)

The third component of the system is the UAV—the **aircraft** itself. As previously mentioned, one of the main incentives behind the deployment of UAVs is removing pilots from physical harm when operating in various war theaters. For this reason, UAVs can be operated in a space that is thousands of miles away from the location of their operators. However, by not being in the cockpit, operators are forced to trust the data they receive from the UAV transmissions. UAVs are therefore equipped with both aperture and infrared cameras that enable operators to direct them and monitor the terrain below them even in harsh meteorological conditions.[14] In other words, these cameras act as the operator's eyes, gathering information and subsequently projecting this information through images on computer screens in front of their operators who rely on the continuous and live optic feed before them to maneuver the UAV. The high resolution of the cameras with which UAVs are equipped and the fact that the images are being live-streamed creates a situation potentially vulnerable to exploitation. For instance, the Gorgon Stare and ARGUS systems respectively consist of twelve and ninety-two high resolution cameras that can be installed on UAVs to upgrade their less sophisticated standard camera.[15] Given that the very high quantity of images captured by the Gorgon Stare or ARGUS can overwhelm the operator tasked to monitor them, it could be nearly impossible for the operator to know if the UAV has been targeted by a cyberattack, underscoring the system's vulnerability.

Mapping the Different Plausible Cyberattacks on UAV Systems

Since UAVs are technologically complex machines, perhaps the "easiest" way for an adversary to attack UAVs is not to emulate them but rather to exploit the weaknesses within their architecture. Moreover, the United States has is deploying its UAVs in the last two decades primarily against non-state actors such as terrorists mostly in situations of "air superiority." Given this competitive advantage, the actors seeking to attack UAVs will

[14] Ibid.

[15] See Noah Shachtman, "Air Force to Unleash 'Gorgon Stare' on Squirting Insurgents," *Wired*, February 19, 2009, accessed December 30, 2016, https://www.wired.com/2009/02/gorgon-stare/.

find doing so via kinetic means more difficult than if they too possessed sophisticated weaponry. Consequently, a likely alternative for non-state actors is to exploit its architecture, which can sometimes be done with very limited resources (table 1 lists the different kinds of plausible cyberattacks targeting a UAV system).

While fully commandeering a UAV—as sea pirates would upon successfully boarding a vessel—represents a cyberattack that requires a high degree of sophistication, gaining *some* "access" to UAVs is relatively uncomplicated given their reliance on computer networks. The most vulnerable component of the unmanned aerial system is the satellite connection between the aircrafts and the command and control center with which they are in contact. In fact, the aircrafts and communication datalink can be accessed—and indeed exploited—by hackers who strive to steal valuable intelligence. For instance, the US military documented several cases of insurgents who accessed the video feed of Predators.[16]

[16] Siobhan Gorman, Yoshi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected," *Wall Street Journal*, December 17, 2009, accessed January 1, 2017, http://www.wsj.com/articles/SB126102247889095011.

Table 1: Cyberattacks targeting UAV systems and required abilities to conduct them[17]

Type of cyberattack	**Attacked component / UAV type**	**Actors possessing the minimum required ability[17]**	**Historical examples**	**Likely defense options**
Access video feed	Satellite datalink; ISR and armed	Individuals	Insurgents against Predators United States and United Kingdom against Israel	Encrypt datalink
Access video feed and DoS attack	Satellite datalink; ISR and armed	Individuals or terrorist organizations	None recorded to date	Encrypt datalink
Access video feed and swap RCA's video	Satellite datalink; ISR and armed	Corporations	None recorded to date	Encrypt datalink
GPS spoofing	Satellite datalink; ISR and armed	States	Allegedly, Iran against RQ-170 Sentinel	Cryptography, signal-distortion detection, and/or direction-of-arrival sensing
Hack computers controlling RCAs	Command and control center	States	Key logger virus at Creech Air Force Base	Air-gap command a control center; restrict use of removable drives; restrict use of outer technologies (e.g., smartphones or private laptops near or inside the command and control center)

[17] This category includes four types of actors. In increasing order based on the resources available to them in carrying out cyberattacks, they are individuals, terrorist organizations, corporations, and states. The reader should note that this category represents an estimated *minimum* threshold; that is, a cyberattack that can be performed by an individual will also be available to terrorist organizations, corporations, and states as they tend to possess more resources than individuals. However, a cyberattack that can be performed by a state will not be accessible to individuals, terrorist organizations, and corporations, which have fewer resources.

Peter W. Singer and Allan Friedman explain that "to pull this trick," the insurgent hackers used nothing more than a laptop computer and "Skygrabber"—Russian-made software that cost $25.95 and was easily available on the web.[18] Skygrabber allowed them to intercept and exploit unencrypted satellite datalinks between UAVs and command and control centers, obtaining hours of video which they then shared with fellow insurgents.[19] Considering that it costs this modest sum to hack a UAV's datalink but millions to safeguard it, Singer and Friedman ask "[whether] the cybersecurity world favor[s] the weak or the strong?"[20] This type of cyberattack may be among the least sophisticated but most worrisome attack to military users. Seeing what the enemy sees can provide the hacker with critical intelligence. For example, by accessing the video feed of the UAV, the hacker can learn about the user's intelligence-gathering capabilities, including the nature and identities of targets as well as ISR practices and routines. Seeing what one's enemy (or friend) sees does not enable one to determine the thinking or strategizing that takes place behind what is seen; however, it certainly helps to anticipate what the user's next move might be and it allows the hacker to stay a step ahead of the user, which can prove decisive on the battlefield.

Another, more sophisticated instance of UAV cameras being accessed surreptitiously was recorded by *The Intercept*. According to Cora Currier and Henrik Moltke, several Israeli UAVs—including the Hermes and Herons—have been hacked by American and British intelligence agencies.[21] As they explain, the United States' National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ) established a base in Cyprus from where the two countries intercepted the signal of Israeli UAVs and successfully collected video footage, which they used to monitor Israel's activities in Gaza and the West Bank. Currier and Moltke add that this joint secret program, named "Anarchist," allowed the Americans and the British to track the flight path of Israeli UAVs. The

[18] Singer and Friedman, *Cybersecurity*, 260–261.

[19] Gorman et al., "Insurgents Hack."

[20] Singer and Friedman, *Cybersecurity*, 260.

[21] Cora Currier and Henrik Moltke, "Spies in the Sky: Israeli Drone Feeds Hacked by British and American Intelligence," *The Intercept*, January 29, 2016, accessed May 25, 2017, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/.

ability to track Israeli UAVs suggests that the United States and the United Kingdom likely could identify both the location of the Israeli launch-and-recovery station, as well as the command and control center.

The fact that insurgents or states can access the camera of a UAV and see what the UAV sees indeed is a vulnerability, as explained above; however, the ramifications would be far more significant if the hacker gains access not only to the camera but also to the UAV controls. For instance, a mere denial of service (DoS) attack could lead the operator to lose sight of a target for just long enough to allow the target to escape. Depending on the moment at which it is performed (e.g., immediately before taking off or landing of the UAV), such an attack could also result in the crash of the UAV, for a "blind" operator may be unable to avoid nearby obstacles. Insurgents would have a strong incentive to conduct a DoS attack when seeking to escape a UAV hovering above them. The longer the duration of the DoS attack, the more time insurgents would have to leave the area over which the UAV is loitering.

A cyberattack that targets the datalinks connection may corrupt the video feed to lead operators astray. This scenario has been depicted in many films where an individual or an organization hacks into a computer system and into surveillance cameras connected to the system and plays a different footage (sometimes a looping of the sites) with nothing abnormal happening so that those monitoring the cameras will not know that they are being fooled. A parallel can be made between UAVs and this typical movie scenario because UAV cameras are the only medium through which the operator can see what is happening. Thus, if a hacker manages to hack into a UAV's camera—as the above Skygrabber demonstrates—and sends back a looped video influencing the operator to think that the UAV is hovering over a desert, the operator may not realize that they are not actually looking at what the UAV is really seeing. In sum, misdirection could compromise missions and beyond that.

Satellite datalinks make the UAV system's architecture vulnerable for another important reason, namely because they are the channel through which GPS data is passed from the UAV to the command and control center. In so-called "spoofing" attacks, which are similar to the abovementioned movie scenario, the hacker could hack into the GPS transmission and mislead the UAV and its operator into believing that it is somewhere that it is not. A notable instance of this kind of cyberattack took place in 2011 when

Iran allegedly spoofed the GPS of a stealth RQ-170 Sentinel.[22] In fact, Iran claimed that it hacked into the GPS of one of the American UAVs, co-opting it into switching on its auto-pilot mode and then sending it different GPS coordinates that ultimately led it to land in Iran.[23]

Although many specialists have raised doubts about Iran's ability to pull off this type of hack,[24] GPS expert Richard Langley maintains that "it's theoretically possible to take control of a drone by jamming the P(Y) code and forcing a GPS receiver to use the *unencrypted* [original emphasis], more easily spoof able C/A code to to [sic] get its directions from navigational satellites."[25] The "coarse acquisition" or C/A code represents the signal used by all GPS to transmit information to satellites. C/A codes are unencrypted and therefore easier to decode. The "precise" or P code is simply a more powerful and more accurate version of the C/A code and fulfills the same function. The "(Y)" is added after the P to denote that the precise code is encrypted, with an encrypted signal being more secured than an unencrypted one.

While the hacker could not necessarily decrypt the GPS data transmitted under the P(Y) code, due to its encryption, the hacker could overwhelm its signal and compel it to switch to the C/A code, which is not encrypted. Once on the C/A code, the now unencrypted data emitted by the GPS could be intercepted, as with the Skygrabber-based attack mentioned above. Thus, while there is a chance that Iran did not actually hack into the RQ-170 Sentinel in 2011, the possibility of other actors doing so does exist—provided they possess sufficient technological know-how. Given their degree of sophistication, the ability to carry out spoofing attacks is likely held by only a handful of a *state* actors.[26]

[22] Adam Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible," *Wired*, December 16, 2011, accessed January 2, 2017, https://www.wired.com/2011/12/iran-drone-hack-gps/.

[23] Ibid.

[24] See David Axe, "Nah, Iran Probably Didn't Hack CIA's Stealth Drone," *Wired*, April 24, 2012, accessed January 2, 2017, https://www.wired.com/2012/04/iran-drone-hack/; Rawnsley, "Iran's Alleged."

[25] Rawnsley, "Iran's Alleged."

[26] Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS from Spoofers is Critical to the Future of Navigation," *IEEE Spectrum*, July 29, 2016, accessed July 30, 2017, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

At the time of writing, "cryptography," "signal-distortion detection" and "direction-of-arrival sensing" are the three defense mechanisms that are able to mitigate GPS spoofing attacks.[27] Relying on the experimental data they obtained by detecting spoofing attacks against the navigating GPS of a super yacht, Mark L. Psiaki and Todd E. Humphreys note that these complex defense mechanisms may not be sufficient to protect against a spoofing attack if used individually, yet they increase the likelihood of a successful defense when deployed conjointly.[28] That being said, some of these mechanisms may not be suited to the RQ-170 Sentinel or other stealth UAVs. This is because the addition of some defense systems to the UAV could undermine its "stealthiness" unless the system is equipped with the same stealth technology as the aircraft itself. If it is not stealthy, the added defense would be detectable by enemy radars, thereby defeating the main purpose of the stealth UAV.

In addition, considering that the RQ-170 Sentinel is one of the United States' most secret and technologically advanced UAVs at the time of writing, these theoretical eventualities further underscore the architectural vulnerability of the country's UAVs.[29] As mentioned above, Predators and Reapers may still not be using encrypted datalinks, unlike the Sentinel, which makes them even more susceptible to GPS spoofing attacks. Beyond the strategic value of seeing what their enemy sees, hackers would have an incentive to conduct such attacks when a UAV is hovering near an area they consider of importance. The incentive would be even stronger with armed UAVs if the hacker believes that by being inactive, the UAV would strike a militant hideout that the hacker is trying to protect. In such a case, a mere DoS attack might not be sufficient because, unlike militants who can try to flee when being chased by an UAV, physical infrastructure—such as a hideout or training camp—might not be easily and rapidly relocated, if at all.

While satellite datalinks connecting UAVs to command and control centers are vulnerable elements of the UAV system's architecture, the command and control centers are also susceptible to cyberattacks given that they operate exclusively over computer networks. That they are protected by air gaps

[27] Ibid.

[28] Ibid.

[29] While the US Air Force (2009) website features a fact sheet page for the RQ-170 Sentinel, no technical data regarding the aircraft's capabilities and key features is publicly available, in contrast to the MQ-1B Predator and MQ-9 Reaper.

has not prevented malware from infecting these networks, as evidenced by the presence of a key logger virus that infiltrated the military computer systems at Creech Air Force Base in 2011.[30] A private network is said to be protected by an air gap when it is disconnected from the surrounding public networks. This is done to ensure that the network is secured and cannot be accessed through any of the nearby public networks. In other words, the air gap isolates the private network (i.e., the network used at the command and control center) so that the hacker will only be able to hack into the network via physical access to the computers connected to that private network, thereby making it more challenging for the network to be compromised. Publicly available information on the specific virus that targeted Creech Air Force Base has not been released, which makes it difficult to determine exactly how it affected the computer network at the base; however, it is believed that the virus reached the network via removable drives that were inserted by the UAV operators themselves and since then are no longer used by the US military.[31]

This event demonstrates the vulnerability of the human factor.[32] That is, even though their bodies may no longer be present on the battlefield, operators remain at risk of being used by hackers to gain unauthorized access to the system. This can have a wide range of operational implications. A simple infection of the network by a virus could disseminate classified data gathered by UAVs to malicious actors. A more sophisticated malware attack could send unofficial commands to UAVs while it tells the monitors in front of the operators that everything is happening the way it should, somewhat in the manner of the "Stuxnet worm" that struck Iranian uranium enrichment

[30] See Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *Wired*, October 11, 2011, accessed January 2, 2017, https://www.wired.com/2011/10/virus-hits-drone-fleet/.

[31] Ibid.

[32] While attacks based on the human factor may prima facie appear less sophisticated as they do not involve technologically advanced knowledge, their potential effects should not be understated. In fact, the highly-mediatized ransomware WannaCry—reportedly reaching "tens of thousands" of computers in no less than "74 countries" on May 12, 2017 alone—exploited a vulnerability within Microsoft Windows for which a security update had been available since March 14, 2017 (see Microsoft 2017); yet the people sitting in front of those infected computers had failed to install it.

facilities in 2009.[33] While the cyber component of these types of attack need not be elaborate, they remain quite sophisticated overall because they first require physical access to the command and control center, a step that might prove cumbersome given the high level of physical security surrounding these sites.

Although attacks targeting the command and control center are comparatively more difficult to carry out, as explained above, hackers have significant incentives in launching them given the strategic value of successful attacks. For instance, by implanting highly sophisticated malware into the command and control center, the hacker could create a kinetic effect on the UAV by issuing malware commanding an armed UAV to fire its missiles at the wrong targets. Moreover, the malware could cause the UAV's missiles, which contain small computers that are also subject to cyberattacks, to be dysfunctional or even detonate while still on the UAV, thus destroying the aircraft. Given that they often lack the ability to conduct air-to-ground attacks, terrorist organizations would have an incentive to conduct cyberattacks that would enable them to gain some control over a UAV's payload, which they could use as if it were their own. The cyberattack possibilities here are endless and cannot be addressed comprehensively. Yet, stressing their plausibility should be sufficient to alert the reader (as well as UAVs users) of their potential threats.

Regardless of which type of attack is pursued, hackers have an incentive to design malware that will take a long time before being noticed so that they can exploit the system as long as possible. In fact, a Department of Defense official puts it this way: "For a sophisticated adversary, it's to his advantage to keep your network up and running. He can learn what you know. He can cause confusion, delay your response times—and shape your actions."[34] And since UAVs have gained such an important position at the center of the US military's arsenal, the "prize" for hacking them becomes even more valuable, perhaps even more than shooting them down from the sky. In other

[33] See Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, accessed January 2, 2017, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[34] Quoted in Nathan Hodge and Noah Shachtman, "Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)," *Wired*, December 17, 2009, accessed January 2, 2017, https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

words, the more powerful and effective the weapon is, the more coveted it will become for actors hoping to gain operational advantage.

Conclusions and Policy Recommendations

UAVs are now at the center stage of many of the major world powers' counterterrorism campaigns, including the United States, Israel, and the United Kingdom. Referencing a 2014 Rand Corporation assessment, Kreps notes that "China, India, Iran, Russia, Taiwan, Turkey, [and] the United Arab Emirates" are currently developing their own UAVs.[35] She goes on, saying that "the world is becoming awash with drones and the indications are that these are not only here to stay, but to spread."[36] The subject of UAVs is therefore becoming very important and relevant for all states using them for military purposes.

As UAV systems become entrenched within the militaries, the cyber threats posed to those systems have also become more frequent and from various types of adversaries, as this paper has highlighted; yet, as was explained above, not all adversaries are able to carry out all kinds of plausible cyberattacks on UAVs. An important part of mitigating these threats begins with an awareness of their existence, which is the aim that this paper sought; simply being aware of a vulnerability is not enough, however, and additional steps must be conducted in order to alleviate the potential damage that the cyberattacks can engender for the user of UAV systems.

The following three recommendations should be regarded as critical next steps toward addressing the cyber vulnerabilities of UAVs and should ultimately increase their defense system:

1. Users should begin by **assessing the vulnerability** of their systems. This assessment should be based on both the system's architecture—which includes the command and control center, the satellite, and the aircraft—as well as the capabilities of the adversaries or others that have incentives to hack the system.
2. The user of UAVs should create technological back-up solutions than would alert or **indicate that the system has been accessed** by an unauthorized actor and is therefore compromised. In the absence of such an alarm system, the operator cannot detect that a cyberattack has

[35] Kreps, *Drones*, p. 60.

[36] Ibid., p. 160.

taken place or is in the process of being carried out and is less likely to be able to defend against it.

3. More efforts should be made to **encrypt datalinks that transmit information** from one part of the system to another. The user should also devise other protection methods—especially on armed systems—even if they are employed in arenas where the threat is estimated to be lower, as the least sophisticated cyberattacks can still damage the system.

In conclusion, these recommendations undoubtedly come at a cost to the system—both financially and in terms of the system's relative effectiveness. For instance, while encrypted datalinks are more secured, encryption inescapably lengthens the decoding process. However, the potential damage that a successful cyberattack on the UAV system could produce likely outweighs the costs. Awareness is key; a realistic assessment of the system's vulnerabilities that does not underestimate the potential damage of a simple cyberattack by an individual, a terrorist organization, or even a state represents an essential first step toward setting up cost-effective defensive measures for UAVs.